SECURITY INTELLIGENCE
REVIEW COMMITTEE

SIRC Report 2000–2001

An Operational Audit of the Canadian Security Intelligence Service

Canada

Security Intelligence Review Committee
122 Bank Street
P.O. Box 2430, Station D
Ottawa, Ontario
K1P 5W5

Tel: (613) 990-8441
Fax: (613) 990-5230
Web Site: http://www.sirc-csars.gc.ca
Collect calls are accepted, and the switchboard is open
from 8:00 a.m. to 5:30 p.m. Eastern Standard Time.
© Public Works and Government Services Canada 2001
Cat. No. JS71-1/2001
ISBN 0-662-65978-3

102-00381/

The Honourable Lawrence MacAulay, P.C., M.P.
Solicitor General of Canada
House of Commons
Ottawa, Ontario
K1A 0A6

30 September 2001

Dear Mr. MacAulay:

As required by section 53 of the *Canadian Security Intelligence Service Act*, we transmit to you the Report of the Security Intelligence Review Committee for the fiscal year 2000–2001, for your submission to Parliament.

Yours sincerely,

Paule Gauthier, P.C., O.C., O.Q., Q.C.
Chair

James Andrews Grant, P.C., Q.C

Robert Keith Rae, P.C., O.C., Q.C.

Raymond Speaker, P.C., O.C.

Frank McKenna, P.C.

Contents

Statement from the Committee vii

How SIRC's Annual Audit Report is Organized x

Section 1: Review of CSIS Intelligence Activities 1

A. **Areas of Special Interest for 2000–2001** 3
CSIS Liaison with Foreign Agencies 3
Ministerial Direction, Revised and Updated 7
Domestic Exchanges of Information (5) 9
Review of Warrant Preparation 11
Security Screening Briefs to Citizenship and Immigration Canada 12

B. **Annual Audit of CSIS Activities in a Region** 15
Targeting of Investigations 15
Warrant Implementation 17
Audit of Sensitive Operations 18
Internal Security 19

C. **Inside CSIS** 20
Warrants and Warrant Statistics 20
CSIS Operational Branches 22
Arrangements with Other Departments and Governments 24
Collection of Foreign Intelligence 26

Section 2: Security Screening and Investigation of Complaints 29

A. Security Screening 31

B. Investigations of Complaints 35

Section 3: CSIS Accountability Structure 39

A. Operation of CSIS Accountability Mechanisms 41

B. Inside the Security Intelligence Review Committee 43

Appendix A: Abbreviations 47

Appendix B: SIRC Reports and Studies Since 1984 51

Appendix C: Major Findings and Recommendations 61

Appendix D: Complaint Case Histories 67

Statement from the Committee

The events of September 11, 2001 in the United States will have put to rest any lingering doubts that the most serious threats to Canada's security and the safety of its citizens come in forms sharply different from those of an earlier generation. Some sixteen years ago when the country's security intelligence apparatus was last overhauled, the singular military politics of the Cold War were of preeminent concern. Today we all live in a world characterized by different and diverse forces, all in rapid flux.

People, capital, information, technologies and political ideologies are more mobile than ever before. The resulting influences are mostly welcome or at least benign, but others are decidedly not. And as a democratic country that encourages international contact and investment and welcomes visitors and immigrants, Canada opens itself to both the best and the worst of these influences.

This sea change in the nature of the threats is reflected wherever public policy touches on Canada's national interests and the safety and security of its citizens:

- At the level of Ministerial Direction to the nation's security intelligence community, politically motivated violence and terrorism are clearly identified as being the most serious threats to Canada and Canadians.
- The deployment of resources within the Canadian Security Intelligence Service, whether measured in person years or budget allocation, reflects the growing need to meet multiple terrorist threats.

- The Service's recent public annual reports are heavily weighted towards concerns about terrorism and an international security environment that makes it easier for terrorist activities to take place in Canada and abroad.
- Proposed and actual changes in legislation brought forward by the federal government (Bill C-16, an amendment to the *Income Tax Act*; and Bill C-11, an amendment to the *Immigration Act*) are both expressions of concern about politically motivated violence being directed or funded from within Canada.
- Parliament's most recent inquiry into security intelligence matters, the 1999 *Report of the Special Senate Committee on Security and Intelligence* (Kelly Report), was almost entirely taken up with the issues of terrorism and political violence and devoted little attention to espionage threats.

In short, CSIS has been transformed in a mere decade from a primarily anti-espionage organization working to block the intelligence-gathering activities of a fairly limited number of foreign governments into one in which terrorism and the politics accompanying it have become dominant.

This transformation is manifest in complex ways. Increasingly, the Service's "case load" involves the need to make nuanced judgements about politically motivated organizations and individuals—nuanced because the line between legitimate, political activity and illegitimate actions involving violence or threats of violence is frequently blurred. Because it is the Committee's task to review and assess the quality of the Service's judgements on these matters, as CSIS's priorities have shifted, so have our own.

The Service's "case load" involves the need to make nuanced judgements about politically motivated organizations and individuals

Issues of legitimate versus illegitimate political activity and what constitutes "association" with a terrorist organization are taking on ever greater importance for the Committee in its review and complaints/tribunal functions. In both areas, the Committee's work has been fundamentally transformed from that of 15 or even 10 years ago and will evolve still further.

Terrorist threats, originating from new and divergent sources, put a premium on understanding developments across the globe as they unfold. As CSIS redirects its efforts, the Committee will continue to adjust its research focus and resources accordingly.

The complaints and tribunal side of the Committee's operations have seen considerable change as well. A rising proportion of complaints involve issues of immigration and security screening, most of which turn on Service assessments of politically motivated individuals and require lengthy inquiries into activities, intelligence sources and political cultures in other countries. Should Bills C-16 and C-11 come into force, the Committee expects the number of similar complaints to increase still further.

The Committee does not believe there is a magic policy or legislative remedy that will make these judgements any less fraught or the appropriate balance between national security and the protection of civil rights any easier to locate. Existing national policy instructs the Service to investigate those threats it believes the Government needs to know about, based on its professional assessment of the seriousness of the threat. SIRC's assessments are similarly grounded in professional experience and knowledge, rather than in policy manuals. Nor does the Committee believe that precise definitions of "terrorist" or "association" or "extremism" would be very helpful, especially in a global environment where the velocity of change seems to increase daily.

The Committee does not believe there is a magic policy that will make these judgements any less fraught

However, SIRC does bring a special perspective to the dilemmas of security intelligence—just as Parliament intended. CSIS represents a government's right and responsibility to protect the lives of citizens, and to preserve law and order. SIRC, *inter alia*, embodies a legal principle at the core of Canadian democracy, namely that citizens have rights to privacy, civil liberties and freedom from untrammelled government power—the "liberty of the subject."

The complexity and ambiguity that have come to dominate security intelligence work means that an ever larger part of the Service's powers of judgement—and, therefore, those of the Committee—are focussed on decisions vital to preserving both Canadians' liberty and their security. Terrorism is an affront to democracy; confronting it will require both greatly increased international cooperation and strength of purpose, and an ongoing commitment to Canada's core values.

How SIRC's Annual Audit Report is Organized

The report is organized to reflect the Committee's primary functions: first, to review CSIS intelligence activities, second, to investigate complaints about CSIS and associated matters and third, to act in concert with other parts of the governance system to protect Canadians from threats to their security.

- Section 1 presents the Committee's review and audit of what the Service does and how it does it. The subsections represent the different methods the Committee employs to make these assessments.

- Section 2 deals with the Committee's role as a quasi-judicial tribunal with the power to investigate complaints of various kinds.

- Section 3 brings together under one heading—CSIS Accountability Structure—the Committee's review of the multiple administrative and legal mechanisms that hold the Service accountable to Government, Parliament, and the people of Canada.

As before, the report draws a clear distinction between Committee comments, observations and recommendations bearing directly on our major task—reviewing CSIS and associated activities for a certain period—and the more general background material we are making available with the aim of assisting Canadians and other readers to understand the context in which security and intelligence work is carried on.

Subjects the Committee believes will be of historical, background or technical interest to readers are set apart from the main text in shaded insets. Unlike the main body of the report, they do not reflect Committee opinion or conclusions as such and are intended to be factual in nature.

Each section of the audit report is labelled with the SIRC study from which it is abstracted. The full references are found in Appendix B.

Section 1

Review of CSIS Intelligence Activities

Review of CSIS Intelligence Activities

A. Areas of Special Interest for 2000–2001

CSIS Liaison with Foreign Agencies

Report #2000-03

BACKGROUND

As stipulated in section 38(a)(iii) of the *CSIS Act*, SIRC reviews arrangements entered into by CSIS with foreign intelligence and police agencies and monitors the flow of information to agencies with which CSIS has co-operation and information-sharing arrangements.

This year, the Committee audited a Security Liaison Officer (SLO) post overseas that operates in an especially difficult working environment. Maintaining the security of the physical operating environment is a continual, major challenge and the situation is compounded by generally onerous working conditions.

CSIS opened the post in the belief that constructive engagement through dialogue and information exchanges would assist the Service in addressing its national security mandate. The Service has sought out specific areas of common ground in which the information exchanged can serve Canadian interests and characterizes its approach to the relationship as "cautious" and "measured"—one that encourages transparency and co-operation.

METHODOLOGY OF THE AUDIT

The Committee's review encompassed three categories of material:

- all exchanges of information handled by CSIS SLOs at the post, including electronic exchanges;
- all correspondence with foreign intelligence agencies handled by the post;
- all instructions and reference materials provided to and originating with the SLOs, including their "Assessments of Foreign Agencies."

The essential goals of the review were to ensure that relationships and contacts with the foreign agencies concerned corresponded to the specific liaison agreements

in place and that information disclosed to foreign agencies or received from them was properly handled by the Service.

More broadly, the Committee examined the activities of the selected post in the context of the Service's overall foreign liaison program, including Ministerial Direction and the Service's policies. As it has during previous reviews of CSIS foreign liaison activities, the Committee paid special attention to any information exchanges that might potentially result in abuses of human rights by other parties.

POLICIES AND ADMINISTRATION

Foreign liaison policies are set out in Ministerial Direction. The relevant Direction, for the period under review, was issued in 1982. As prescribed by section 17 of the *CSIS Act*, the Service may enter into individual arrangements with agencies of other countries. These arrangements, which define the intended nature and scope of each co-operative relationship, are reviewed by the Committee.

Establishing liaison arrangements with foreign intelligence services must be approved by the Solicitor General after consultation with the Minister of Foreign Affairs and International Trade. The arrangement governing exchange activities at the post selected for this year's audit was signed during the past decade.

New Ministerial Direction

As noted earlier, the Ministerial Direction relevant to the period under review was drafted in 1982. Since the Committee completed its audit of the selected SLO post, however, a new Ministerial Direction has been issued covering the entirety of CSIS operations, including foreign liaison arrangements. With particular reference to foreign liaison activities, the Committee in its 1997–1998 Report expressed concern about the need for the Government to update its Ministerial Direction and recommended that the Service re-examine all its liaison arrangements to ensure conformity with the new framework once issued. In light of these earlier comments, the Committee in its review of the new Ministerial Direction paid particular attention to those elements that pertain to foreign liaison. (For a full discussion of the new Ministerial Direction, *see* page 7.)

With respect to foreign liaison, the new Ministerial Direction appears to preserve the key policy elements of the earlier document, namely:

- arrangements are to be established as required to protect Canada's security;

- they are to be approved by the Solicitor General after consultation with the Minister of Foreign Affairs and International Trade;
- the human rights record of the country or agency concerned is to be assessed and the assessment weighed in any decision to enter into a co-operative relationship;
- the applicable laws of Canada must be respected and the arrangement must be compatible with Canada's foreign policy.

The one significant departure from earlier Direction is that the new document grants greater discretion to the Director of CSIS to manage the individual co-operative arrangements. Formerly, Ministerial Direction gave the responsibility for setting out the specific parameters of co-operation to the Minister. The new document states that "the Director will manage these arrangements subject to any conditions imposed by the Minister."

Since the new Direction was issued only in February 2001, it will be some time before the Committee can assess the implications of the revised policies, especially as they relate to the Director's increased discretionary authority. However, considered broadly, we believe the new Ministerial Direction is a substantial improvement over the earlier documents because the terminology employed is simpler and is consistent with that used in the legislation that governs CSIS activities as a whole.

The new document grants greater discretion to the Director of CSIS to manage individual arrangements

In the Committee's 1997–1998 review of foreign liaison arrangements, and in anticipation of the new Ministerial Direction, we recommended that the Service systematically re-examine all foreign arrangements in light of the new Direction once it was issued, so as to ensure conformity. The Service has informed the Committee that it will conduct its next yearly evaluation of all liaison relationships within the framework of the new Direction.

FINDINGS AT THE POST

Overview

During the Committee's audit of the SLO post, we were struck by the substandard conditions in which Service staff were obliged to work. The poor physical facilities

at Canada's mission and an onerous workload, arising from increasingly large numbers of immigration and visa applications requiring security screening, combine to form an adverse environment. Notwithstanding these difficult circumstances, however, the SLO and staff are performing well.

We found that the SLO has made steady progress with foreign interlocutors; however, rising demands from the immigration side of the SLO's mandate left less time for developing relationships with other countries in the region for which the post is nominally responsible.

Screening Activities

The Committee's review of the post's resource allocation showed a growing share of staff time being devoted to immigration and visa security screening. In a matter of a few months the immigration/visa screening workload had risen dramatically, to the extent that additional Service personnel were temporarily detailed to the post to provide assistance. Poor physical facilities and the challenging security environment complicated matters further.

> We were struck by the substandard conditions in which Service staff were obliged to work

The evident work overload gave rise to concerns on the part of the Committee that some of the post's important functions might not be being handled expeditiously. Service senior management told the Committee that it shared our concerns and believed that the immigration workload problem extended to certain other of its SLO posts as well.

In the early 1990s, CSIS and another federal agency jointly conducted a review of the immigration-related duties at posts abroad, which resulted in more focussed use of CSIS officers' services. It is the Committee's view that the Service might wish once again to review this element of its Foreign Liaison Program. For its part, the Committee intends to conduct audits of security screening functions at selected SLO posts abroad during the course of upcoming reviews.

Information Exchanges

The Committee examined all documentation associated with operational co-operation and information exchanges involving the SLO post from March 31, 1998 through June 30, 2000. The Service's exchanges of information with the foreign agencies covered by the post were reviewed to ensure that the information disclosed to the foreign agencies or received from them was handled properly.

Our review identified only one problematic exchange. Information that tended to cast aspersions on a certain individual—but which in the Committee's view was of doubtful reliability—had been passed on to Service clients. After bringing the matter to the attention of CSIS, we were provided with additional, clarifying information. We advised the Service that it should consider giving this new information to its clients so that the earlier advice would be regarded in its proper context.

Foreign Agencies and Human Rights

Concerns about potential impacts on human rights figured significantly in the Committee's audit of this particular post. Balanced against these concerns was the basic imperative for having arrangements with foreign intelligence agencies in the first place—the need for CSIS to collect information that protects Canadians.

On several occasions in recent years the Committee has expanded on its position regarding CSIS liaison with foreign agencies. We believe the Service should take all possible care to ensure that the information it provides is not used to assist in the violation of human rights. To that end, SLOs are obligated to give the rest of the Service timely and accurate assessments of an agency's human rights record and of its propensity to pass information on to third parties without authorization. The Service must avoid situations in which it gives information to an agency that does not violate human rights, only to find that the data have been passed on to other organizations that do.

With respect to the SLO post under review, the Committee identified no information exchanges that failed to conform to these standards. It is satisfied that all human rights assessments of agencies were properly carried out.

Ministerial Direction, Revised and Updated

In February 2001, the Solicitor General issued a revised compendium of Ministerial Directions governing control and management of the Service—a development the Committee has looked forward to for some time.

THE EVOLUTION OF MINISTERIAL DIRECTION

Section 6 of the *CSIS Act* states that the Director of CSIS has the "control and management" of the Service under the direction of the Minister—specifically, the Solicitor General of Canada. The principal mechanism by which this direction is given is through written instructions or "Ministerial Direction." The Act stipulates

that the Committee be provided with copies of such directions "forthwith" after they are issued.

Ministerial Directions govern a wide spectrum of Service activities ranging from strategic policy, to guidance on specific matters such as the conduct of investigations involving sensitive institutions. In past reviews, the Committee has examined the adequacy of particular Directions, the ways in which the Service has interpreted Ministerial Directions through its own policies and procedures and how the Directions were implemented in individual cases.

Of recurrent concern to the Committee has been the disparate and patchy nature of Ministerial Directions when viewed as a whole. Over the course of the Service's 17-year history, individual ministers often issued Directions on specific matters as and when they arose. Some Directions, which are still valid as Ministerial guidance, actually predate the creation of the Service. The result has been a hodgepodge of policy guidance employing sometimes contradictory language and using terminology no longer consistent with legislation.

Ministerial guidance is streamlined, consistent in its use of language and presented in a cohesive document

NEW DIRECTION: AN OVERVIEW

The new compendium (a classified document), which replaces the old Direction in its entirety, goes a long way to rationalizing the Government's strategic guidance of the Service and, in the Committee's view, reflects a maturation of the legal and policy framework that governs the Service's work. Ministerial guidance is now considerably streamlined, consistent in its use of language and presented in a concise and cohesive document.

It is too soon to assess the effect of the revised Directions on the Service's operations. However, the compendium's relative brevity and the strategic nature of the direction given suggests that there will be an increased focus on the Service's own Operational Policies as the source for specific instructions and guidelines for implementation. Also apparent is an overall shift in discretionary powers from the Office of the Solicitor General to the Director of CSIS, with respect to the day-to-day management of the Service. In the course of future audits, the Committee intends to pay particular attention to how the new guidance is interpreted and implemented across the range of CSIS activities.

Domestic Exchanges of Information (5)

Report #2000-01

BACKGROUND

In carrying out its mandate to investigate suspected threats to the security of Canada, CSIS co-operates and exchanges information with federal and provincial departments and agencies and police forces across Canada. Section 17 of the *CSIS Act* sets out the Service's mandate to enter into these arrangements. Section 19(2) of the Act allows CSIS to disclose information to various domestic departments and agencies "for the purposes of the performance of its duties and functions."

The Review Committee is charged, under section 38(a)(iii) of the Act, with the task of examining the co-operative arrangements the Service has with domestic agencies, as well as the information and intelligence it discloses under those arrangements.

AUDIT SCOPE AND METHODOLOGY

The Committee examined all Service exchanges of information, including incidental disclosures, with other domestic agencies for the fiscal year 1999–2000. In addition, the Committee conducted an on-site review of information exchange practices in one Service regional office.

The purpose of the review was to determine whether the Service exchanged information with domestic bodies in conformity with Ministerial Direction, existing Memoranda of Understanding (MOU) with government institutions and police services, CSIS operational policies, the *CSIS Act* and other relevant statutes. In particular, the Committee's enquiries sought to determine if:

- the threat necessitating the exchange sufficiently outweighed the public's reasonable expectation of privacy;
- the exchange of information was strictly necessary to meet the Service's operational requirements as per section 12 of the *CSIS Act*;
- the exchange of information involved the unnecessary use of personal and sensitive information;
- the information exchanged was reasonable and factually accurate;
- all disclosures of information by CSIS to other bodies accorded with the limitations set out in section 19(2) of the *CSIS Act*;
- all exchanges of information were tracked in a consistent manner.

COMMITTEE FINDINGS

Overall co-operation

For the period under review, the Committee identified two information exchanges that raised concern. All others complied with the Service's mandate and conformed to existing policy. The information exchanged was reasonable and accurate and did not involve the unnecessary use of personal and sensitive information, nor did it infringe unduly on personal privacy.

Retention of unsolicited information

The two cases that drew the Committee's attention both arose from our on-site audit of a CSIS regional office and involved how information received from domestic agencies was managed.

In the first case, the Service's database holding the unsolicited material contained several items relating to individuals and organizations for which CSIS did not have targeting authorizations. We asked the Service to explain its reasons for retaining this material and were satisfied with the explanation. The Committee believes that in future, however, the rationale for retaining unsolicited information of a similar nature should be clearly set out in the relevant operational reports.

> **The Committee recommends that the purpose for retaining information under a general collection category be clearly identified in operational reports.**

The Service has since concurred with our recommendation and advised that the relevant section of operational policy will be amended accordingly.

The second case that drew our attention concerned the appropriateness of retaining certain information received from a domestic agency. The files related to the activities of a small group of minors. The Service told the Committee that it originally retained the material because it showed a propensity on the part of the group to engage in serious violence against persons or property for the purpose of achieving a political objective—a threat that lies within the Service's mandate. CSIS then decided, based on further assessment of the information, that no further action was required; however, it retained the original exchange of information.

The Committee fully recognizes the Service's responsibility to investigate information received from other bodies that appears to fall within its mandate. However, we question the need, in this case, to retain the information once the determination not to investigate further had been made. It is the Committee's view that the information should be deleted from CSIS records.

For its part, the Service reiterated its position on the validity of retaining the information in the first instance and noted that, in continuing to hold the information, it is preserving a formal record of information received and actions taken. The Service did agree to modify the operational reports to reflect the decision it ultimately made that the information warranted no further action on its part.

The Committee recommends that the service employ greater diligence in deciding whether to retain unsolicited information.

Review of Warrant Preparation

Report #2000-05

To obtain warrant powers under section 21 of the *CSIS Act*, the Service prepares an application to the Federal Court accompanied by a sworn affidavit presenting the reasons why intrusive powers are required to investigate a particular threat to the security of Canada. Because properly prepared affidavits are key to the integrity of the process, the Committee periodically reviews a number of warrants selected from among a comprehensive list of all warrants active during the audit period.

Although it is the sole responsibility of the Federal Court to issue a warrant, and to attach whatever conditions it deems appropriate, the Committee's purposes in reviewing the Service's warrant preparation are twofold:

- to ensure that the facts presented in the affidavit are consistent with the information used as the basis for its preparation;
- to ensure that the facts, circumstances and statements of belief contained in the affidavit are presented fairly and objectively.

From among the warrants issued in 1999–2000, the Committee selected two for detailed review; one a counter terrorism target, the other relating to a counter intelligence investigation. The Committee examined all CSIS documents relating to the preparation of the warrant affidavits: working files, "facting" binders, internal messages, Target Approval and Review Committee (TARC) minutes, Requests for TARC Authorities (RTAs) and the affidavits themselves.

In each of the cases selected, the Committee found that the affidavit the Service provided to the Federal Court was factually consistent with the supporting documentation and that the facts and circumstances presented in the affidavit were fairly and objectively expressed.

REVISIONS TO WARRANT CLAUSES AND CONDITIONS

As noted in last year's Report (*SIRC Report 1999–2000*), the Service has undertaken a broad revision of warrant clauses and conditions with a view to simplifying the terminology and bringing it into line with current legislation. Some operational and administrative procedures were also modified.

CSIS has informed the Committee that this process is now complete and that all Service personnel involved either with applying for warrants or implementing them have been fully briefed. All changes reflected in subsequent warrant applications have been approved by the Federal Court of Canada.

Security Screening Briefs to Citizenship and Immigration Canada

Report #2001-02

The aim of this study was to assess the information provided by CSIS to the Minister of Citizenship and Immigration Canada (CIC) in its mandated role to assist the government's immigration monitoring program by supplying security screening services. The Committee last examined the Service's role in immigration in its 1997–1998 Report. Our review this year focussed specifically on the nature and quality of the advice CSIS gave to CIC in the form of written briefs.

METHODOLOGY OF THE AUDIT

For this review the Committee examined 16 of the Service's immigration security screening investigations selected from the 166 briefs sent by CSIS to CIC in the 1999–2000 fiscal year. The sample consisted of nine inland cases and seven overseas-based cases. The Committee reviewed the briefs sent to CIC and all supporting documents relevant to each investigation.

HOW THE SERVICE PROVIDES ADVICE

CSIS has the sole responsibility to provide security screening assessments for immigration applications originating in both Canada and the US. For immigration applications originating elsewhere, it is up to the Immigration Program Manager at the Canadian overseas mission concerned to request a Service security screening assessment. In either case, regardless of the advice CSIS gives to CIC, the final decision on any potential immigrant's admissibility rests with the Minister of Citizenship and Immigration.

A typical immigration security screening investigation begins when the Service receives a request from either a Case Processing Centre (CPC) in Canada or an

Immigration Program Manager at a Canadian mission overseas. The investigation ends when the Service provides its advice to CIC in one of four forms:

No Reportable Trace (NRT)—a report given to CIC when the Service has no adverse information on the immigration applicant.

Inadmissible Brief—advice provided when the Service has concluded, based on information available to it, that the applicant meets the criteria outlined in the security provisions of section 19 of the *Immigration Act*.

Information Brief—advice provided by CSIS that it has information that the applicant is or was involved in activities as described in the security provisions of the *Immigration Act*, but that it is of the opinion that the applicant does not fall into the class of persons deemed to be inadmissible under the Act.

Incidental Letter—provided to CIC when the Service has information that the applicant is or was involved in non-security-related activities described in section 19 of the *Immigration Act* (for example, war crimes or organized criminal activity) or any other matter of relevance to the performance of duty by the Minister of Citizenship and Immigration, as set out in section 14(b) of the *CSIS Act*.

All the Service briefs to CIC were found to be accurate and adequately supported by the information collected

FINDINGS OF THE COMMITTEE

Nature of the Service's Advice

All the Service briefs to CIC in which the Service rendered an opinion were found to be accurate and adequately supported by the information collected. We identified one instance in which the Service was unable to provide meaningful advice because it lacked sufficient information.

Overall, the Committee noted that the Service prepared more briefs for inland cases than for overseas-based cases, despite the fact that most immigration cases originate overseas. This issue will be examined in a future review.

Essential Statistics

During the year reviewed, the Service conducted 81 650 immigration security screening assessments, most of which resulted in a "No Reportable Trace" (NRT) response. The Service provided 166 briefs to CIC, 109 of which were inadmissible

briefs. The average time the Service needed to process an immigration security screening case that resulted in an information brief was 661 days. For cases generating an inadmissible brief, the average was 644 days. The Service's explanation for the turnaround times is found in Section 2: Security Screening, page 34.

Recent Developments

In the Committee's Report for 1997–1998, we voiced concerns about flaws in procedures for the security screening of refugee claimants in Canada. We expressed the view that the Service could and should play a greater role in assisting CIC's efforts in this area.

"Grounds to Suspect" "Grounds to Believe" Threats to Security and Inadmissibility in Canadian Law

The security screening assistance rendered by the Service takes the form of information sharing with CIC on matters concerning threats to the security of Canada, as defined in section 2 of the *CSIS Act*, and advice to CIC with respect to the inadmissibility classes in section 19 of the *Immigration Act*. These are separate Acts of Parliament and they contain distinct provisions—"threats to the security of Canada" and "inadmissibility to Canada"— each of which are brought to bear on immigration security issues.

An individual applying for immigration to Canada may be deemed inadmissible in accordance with criteria set out in section 19 of the *Immigration Act*. However, any individual (immigration applicant or otherwise) may also meet the criteria for being a threat to the security of Canada as defined in the *CSIS Act*.

The threshold for inadmissibility under the *Immigration Act* is higher than that for commencing an investigation under section 12 of the *CSIS Act*. To target an individual for a section 12 investigation the Service must have reasonable grounds to "suspect" that a person or a group poses a threat to the security of Canada. By contrast, for CIC to refuse admission for security reasons the Service's inadmissibility brief must help support its conclusion that there are reasonable grounds to "believe" that the applicant is a member of a class of inadmissible persons—a stricter standard to meet under the law.

In its briefs to CIC, the Service provides an assessment of an applicant's admissibility with reference to the *Immigration Act*. However, the Service's role in the process is not to provide advice on whether the applicant poses a threat to the security of Canada as defined in the *CSIS Act*.

briefs. The average time the Service needed to process an immigration security screening case that resulted in an information brief was 661 days. For cases generating an inadmissible brief, the average was 644 days. The Service's explanation for the turnaround times is found in Section 2: Security Screening, page 34.

Recent Developments

In the Committee's Report for 1997–1998, we voiced concerns about flaws in procedures for the security screening of refugee claimants in Canada. We expressed the view that the Service could and should play a greater role in assisting CIC's efforts in this area.

"Grounds to Suspect" "Grounds to Believe" Threats to Security and Inadmissibility in Canadian Law

The security screening assistance rendered by the Service takes the form of information sharing with CIC on matters concerning threats to the security of Canada, as defined in section 2 of the *CSIS Act*, and advice to CIC with respect to the inadmissibility classes in section 19 of the *Immigration Act*. These are separate Acts of Parliament and they contain distinct provisions—"threats to the security of Canada" and "inadmissibility to Canada"— each of which are brought to bear on immigration security issues.

An individual applying for immigration to Canada may be deemed inadmissible in accordance with criteria set out in section 19 of the *Immigration Act*. However, any individual (immigration applicant or otherwise) may also meet the criteria for being a threat to the security of Canada as defined in the *CSIS Act*.

The threshold for inadmissibility under the *Immigration Act* is higher than that for commencing an investigation under section 12 of the *CSIS Act*. To target an individual for a section 12 investigation the Service must have reasonable grounds to "suspect" that a person or a group poses a threat to the security of Canada. By contrast, for CIC to refuse admission for security reasons the Service's inadmissibility brief must help support its conclusion that there are reasonable grounds to "believe" that the applicant is a member of a class of inadmissible persons—a stricter standard to meet under the law.

In addition to CIC, the Service provides an assessment of an applicant's admissibility with respect to the *Immigration Act*. However, the Service's role in the process is not to provide advice on whether the applicant poses a threat to the security of Canada as defined in the *CSIS Act*.

The Committee has recently been advised that the Service and CIC have developed the "Front End Screening" program for refugee claimants in Canada. All refugee claimants would at the time of making a claim be subject to a screening process similar to that for applicants for permanent residence. The aim of the program is to prevent persons from being able to enter Canada and remain for an indefinite period of time without undergoing a security screening assessment—a significant risk under the procedures in place at the time of our earlier review.

This and other recent developments in the co-operative relationship between CSIS and CIC will be followed closely by the Committee.

B. Annual Audit of CSIS Activities in a Region

Every year the Committee audits the entire range of CSIS's investigative activities—targeting, special operations, warrants, community interviews and sensitive operations—in a particular region of Canada. Such a comprehensive examination provides insight into how the Service employs the various investigative tools at its disposal and allows the Committee to assess the ways in which Ministerial Direction and CSIS policies are implemented by the operational sections of the Service.

Targeting of Investigations

The targeting portion of the regional audit reviews how the Service applies its duties and functions as set out in sections 2 and 12 of the *CSIS Act*. The day-to-day management of investigations is governed by both Ministerial Direction and CSIS operational policies.

In reviewing the appropriateness of any Service investigation, the Committee uses three main criteria:

1) Did the Service have reasonable grounds to suspect a threat to the security of Canada?

2) Was the level and intrusiveness of the investigation proportionate to the seriousness of the target's threat-related activity?

3) Did the Service collect only that information strictly necessary to fulfill its mandate to advise the Government of a threat?

METHODOLOGY OF THE AUDIT

Seven investigations were selected for this year's audit—five counter terrorism and two counter intelligence. The Committee examined all files and electronic documents associated with each of the seven cases. We interviewed both the regional managers directly responsible for the investigations and supervisory headquarters staff.

FINDINGS OF THE COMMITTEE

Based on the information reviewed, the Committee was satisfied that in all seven cases the Service had reasonable grounds to suspect a threat to the security of Canada. Neither the files and operational messages we examined nor the interviews we conducted gave any indication that the levels of investigation were out of proportion to the perceived threats.

We also reviewed the information collected in all seven cases. In one instance, certain data collected raised concerns as to whether they met the "strictly necessary" test. Although the Service provided an explanation, the Committee was not

Management of Targeting

Target Approval and Review Committee

The Service's capacity to target (or launch an investigation into) the activities of a person, group or organization is governed by policies that rigorously control the procedures and techniques to be employed. The Target Approval and Review Committee (TARC) is the senior operational committee within CSIS charged with considering and approving applications by Service officers to launch investigations. TARC is chaired by the Director of CSIS and includes senior CSIS officers and representatives of the Department of Justice and the Ministry of the Solicitor General.

Levels of Investigation

There are three levels of investigation, with Level 3 being the most intrusive and accompanied by the most stringent legal controls and management challenges. Level 2 investigations may include personal interviews and limited physical surveillance. Level 1 investigations are for short durations and allow CSIS to collect information from open sources and from records held by foreign police, security or intelligence organizations.

Issue-Related Targeting

An issue-related targeting authority allows CSIS to investigate the activities of a person, group or organization that may on reasonable grounds be suspected of constituting a threat to the security of Canada and that are related to, or emanate from, that specific issue.

METHODOLOGY OF THE AUDIT

Seven investigations were selected for this year's audit—five counter terrorism and two counter intelligence. The Committee examined all files and electronic documents associated with each of the seven cases. We interviewed both the regional managers directly responsible for the investigations and supervisory headquarters staff.

FINDINGS OF THE COMMITTEE

Based on the information reviewed, the Committee was satisfied that in all seven cases the Service had reasonable grounds to suspect a threat to the security of Canada. Neither the files and operational messages we examined nor the interviews we conducted gave any indication that the levels of investigation were out of proportion to the perceived threats.

We also reviewed the information collected in all seven cases. In one instance, certain data collected raised concerns as to whether they met the "strictly necessary" test. Although the Service provided an explanation, the Committee was not

Management of Targeting

Target Approval and Review Committee

The Service's capacity to target (or launch an investigation into) the activities of a person, group or organization is governed by policies that rigorously control the procedures and techniques to be employed. The Target Approval and Review Committee (TARC) is the senior operational committee within CSIS charged with considering and approving applications by Service officers to launch investigations. TARC is chaired by the Director of CSIS and includes senior CSIS officers and representatives of the Department of Justice and the Ministry of the Solicitor General.

Levels of Investigation

There are three levels of investigation, with Level 3 being the most intrusive and accompanied by the most stringent legal controls and management challenges. Level 2 investigations may include personal interviews and limited physical surveillance. Level 1 investigations are for short durations and allow CSIS to collect information from open sources and from records held by foreign police, security or intelligence organizations.

Issue-Related Targeting

An issue-related targeting authority allows CSIS to investigate the activities of a person, group or organization that may on reasonable grounds be suspected of constituting a threat to the security of Canada and that are related to, or emanate from, that specific issue.

entirely satisfied with that response. We believe that the information collected did not meet the strictly necessary test, and we were not satisfied that, in this instance, the Service had adhered fully to the existing operational policies and guidelines governing collection.

Warrant Implementation

Under section 21 of the *CSIS Act*, only the Federal Court can grant CSIS the warrant powers required to use the most intrusive investigative procedures available to it, such as telephone or mail intercepts. Every year the Committee reviews how warrants are implemented in a number of cases selected from the files of a particular region.

The Committee's review involves assessing:

- how the Region used the warrant powers granted by the Federal Court;
- whether the Region complied with all clauses and conditions contained in the warrants;
- whether the Region's implementation of the warrants was carried out in accordance with the Act, CSIS policy and Ministerial Direction.

FINDINGS OF THE COMMITTEE

Warrant Implementation

The Committee's review of the selected warrants and the associated investigation files revealed no instances of unnecessary use of warrant powers. All collection activities were carried out in accordance with the clauses and conditions contained in the warrants. However, with respect to the Service's collection and retention of product from certain warrants, the Committee identified possible anomalies in two of the cases reviewed.

All collection activities were carried out in accordance with the clauses and conditions contained in the warrants

In the first, the Committee questioned why the Service retained a particular kind of data beyond the standard period established in CSIS operational policies. In response, the Service advised the Committee that the special retention was authorized so that assistance could be rendered to an allied agency's investigation of a terrorist network.

The second case concerned the intercepting and reporting on the communications of persons not named in the warrant. In both instances where this appeared to have taken place, the Committee subsequently was satisfied with the Service's explanation that both interceptions were appropriate and within the law (one under the provisions of the "basket clause" and the other because the intercepted person qualified as a "Vanweenan"[1]).

Shortage of Special Resources

The Committee's examination of the Region's investigation files showed that the Region suffered from the shortage of a particular expert resource. Although the resulting delays had no adverse effects in the cases we examined, the Committee would not wish to see a delay in processing unduly hinder the timely distribution of important information to appropriate officials. The Committee has expressed similar concerns in the past, and we are encouraged by the Service's initiatives to remedy the situation in this Region.

Audit of Sensitive Operations

Using human sources in collecting information is essential to effectively investigating threats to public safety and national security. However, the sensitivity of such operations is such that they are the subject of special Ministerial Direction. In addition, the procedures for implementing sensitive operations are set out in some detail in the CSIS *Operational Policy Manual*. All requests for sensitive operations, or for investigations involving "sensitive institutions" require the approval of Service senior management.[2]

---

1. The basket clause permits intercepting communications of persons who, while not named in a warrant, may be present at a location named in the warrant. The legality of the clause was upheld by the Supreme Court of Canada in *R v. Chesson*, [1988] 2 S.C.R. 148. Affirmed in the same judgement was the legality of intercepting a person named or described ("spouse" or "colleague", for example) in the warrant but not specifically targeted, likely to have regular contact with the target, and whose communications the investigating agency has reasonable grounds to believe may assist the investigation. The name of one of the parties to the "Chesson" case—Vanweenan—has since come to denote this category of persons.

2. Sensitive institutions are defined as trade unions, the media, religious institutions and university and college campuses.

METHODOLOGY OF THE AUDIT

The Committee reviewed a set of randomly selected human source operations as well as all requests to senior managers involving sensitive institutions. In each instance, we examined all files related to recruiting, developing and directing the human source in question. The purpose of the review was to assure ourselves that in handling human sources and conducting investigations involving sensitive institutions, the Service had complied with the Act, Ministerial Direction and its own operational policies.

FINDINGS OF THE COMMITTEE

With respect to both the Region's development and direction of human sources and its investigations involving sensitive institutions, the Committee concluded that the Service's actions were reasonable, appropriate and necessary for properly fulfilling its mandate.

We did identify, however, an area where the Regional office had not fully complied with Service policies governing certain administrative procedures. The Committee believes that periodic verification by Regional office management could have avoided this administrative shortcoming.

Internal Security

OVERVIEW

The Committee's inquiries showed that, within the Regional office, the level of awareness about security was generally high, and that management had undertaken appropriate measures to ensure vigilance among Service employees. We did observe, however, that the Region had conducted significantly fewer random luggage searches of its employees than CSIS offices in other regions. The Service informed us that for fiscal year 2001–2002, the Region's objective is to conduct luggage searches monthly.

> The breach occurred because the two Service employees involved left their vehicle out of sight and unattended

A BREACH OF SECURITY

The Committee examined the files regarding a security breach case that occurred during the period under review. The breach involved the theft of classified assets and material from an operational vehicle. Our review showed that the Region and

CSIS Headquarters internal security representatives had effectively investigated the incident, and that appropriate remedial measures had been taken to reduce the potential for similar security breaches in the future.

Two matters concerning the case drew the Committee's attention. First, the breach occurred because the two Service employees involved left their vehicle out of sight and unattended, which was, in the Committee's view, a lapse in judgement. Second, although in the wake of the incident the Service subsequently made constructive changes to security policies and procedures, the Committee believes that some unnecessary ambiguities remained that had the potential to weaken the policy overall.

Responding to the Committee's observations, the Service asserted that the breach did not stem from a lapse in judgement, that its employees had taken all necessary precautions and followed all established procedures and, moreover, that no disciplinary actions were contemplated. The Service agreed to adjust its policy manual to reduce the possibility of misinterpretation.

C. Inside CSIS

Warrants and Warrant Statistics

Warrants are one of the most powerful and intrusive tools in the hands of any department or agency of the Government of Canada. For this reason alone their use bears continued scrutiny, which task the Committee takes very seriously. In addition, our review of the Service's handling of warrants provides insights into the entire breadth of its investigative activities and is an important indicator of the Service's view of its priorities.

The Committee compiles statistics quarterly on CSIS warrant affidavits and on warrants granted by the Federal Court. We track several kinds of information annually, including the number of persons and targeted groups subject to warrant powers. Table 1 compares the number of warrants issued over the last three fiscal years.

The Federal Court issued 32 urgent warrants during 2000–2001. No applications for warrants were denied by the Federal Court during the fiscal year under

review, and none of the decisions issued by the Court impacted upon existing warrant powers.

OBSERVATIONS ON WARRANT NUMBERS

Although the data collected by the Committee provide good insight into how the Service exercises its warrant powers in a given year, comparing them between years is more problematic. A range of factors as disparate as court decisions and new developments in technology introduce significant variations into how warrants are applied for and how they are implemented. Even raw warrant numbers can be misleading since a single warrant can authorize the use of warrant powers against more than one person.

Allowing for these factors, however, the Committee concludes that the total number of persons affected by CSIS warrant powers has remained relatively stable for the last 3 years, and that foreign nationals continue to represent the majority of persons subject to warrant powers.

REGULATIONS

Under section 28 of the *CSIS Act*, the Governor in Council may issue regulations governing how CSIS applies for warrants. In 2000–2001, no such regulations were issued.

---

3. A replacement warrant is required when the Service changes the targets, the places or the powers of an existing warrant.

Table 1
New and Replaced/Renewed Warrants

	1998–1999	1999–2000	2000–2001
New Warrants	84	76	56
Replaced/Renewed Warrants	163	181	160
Total	247	257	206

review, and none of the decisions issued by the Court impacted upon existing warrant powers.

OBSERVATIONS ON WARRANT NUMBERS

Although the data collected by the Committee provide good insight into how the Service exercises its warrant powers in a given year, comparing them between years is more problematic. A range of factors as disparate as court decisions and new developments in technology introduce significant variations into how warrants are applied for and how they are implemented. Even raw warrant numbers can be misleading since a single warrant can authorize the use of warrant powers against more than one person.

Allowing for these factors, however, the Committee concludes that the total number of persons affected by CSIS warrant powers has remained relatively stable for the last 3 years, and that foreign nationals continue to represent the majority of persons subject to warrant powers.

REGULATIONS

Under section 28 of the *CSIS Act*, the Governor in Council may issue regulations governing how CSIS applies for warrants. In 2000–2001, no such regulations were issued.

---

5. A replacement warrant is required when the Service changes the targets, the places or the powers of an existing warrant.

CSIS Operational Branches

COUNTER INTELLIGENCE

The Counter Intelligence (CI) Branch monitors threats to national security stemming from the offensive espionage activities of other national governments' intelligence services in Canada.

During the year under review, personnel and other resources were reallocated internally so as to meet what the Service regards as the increasingly complex challenges of the Counter Proliferation and Transnational Criminal Activity areas of CI's mandate. As is the case in other branches of the Service, CI Branch regards as a priority recruiting and retaining personnel with in-depth knowledge of computer and other sciences, international financial markets and other technical specialities. Specialized skills were added to the Branch's capacity through the use of secondees from other government departments.

The Service claimed success in curtailing the activities in Canada of a number of foreign intelligence services through continual efforts at forging constructive liaison relationships. CSIS also pointed to several examples where co-operation with domestic agencies, as well as allied foreign intelligence services, had yielded positive results.

CSIS Role in Preventing Politically Motivated Violence

CSIS plays a pivotal role in Canada's defence against the possible threats posed by groups associated with politically motivated violence. The "threats to the security of Canada," which it is specifically charged to investigate, include "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state . . ." [section 2(c), *CSIS Act*].

In addition to informing the Government in general about the nature of security threats to Canada, CSIS' intelligence and advice is specifically directed at several government departments or agencies. The information can form the basis for immigration screening profiles used in processing immigrants. In specific cases, CSIS advice can play an instrumental role in determining the admissibility of an applicant, or in denying citizenship. Security intelligence may also serve as a basis for determining an individual's suitability to have access to classified information, as well as assisting the police in crime prevention and in criminal prosecutions.

CSIS Operational Branches

COUNTER INTELLIGENCE

The Counter Intelligence (CI) Branch monitors threats to national security stemming from the offensive espionage activities of other national governments' intelligence services in Canada.

During the year under review, personnel and other resources were reallocated internally so as to meet what the Service regards as the increasingly complex challenges of the Counter Proliferation and Transnational Criminal Activity areas of CI's mandate. As is the case in other branches of the Service, CI Branch regards as a priority recruiting and retaining personnel with in-depth knowledge of computer and other sciences, international financial markets and other technical specialities. Specialized skills were added to the Branch's capacity through the use of secondees from other government departments.

The Service claimed success in curtailing the activities in Canada of a number of foreign intelligence services through continual efforts at forging constructive liaison relationships. CSIS also pointed to several examples where co-operation with domestic agencies, as well as allied foreign intelligence services, had yielded positive results.

CSIS Role in Preventing Politically Motivated Violence

CSIS plays a pivotal role in Canada's defence against the possible threats posed by groups associated with politically motivated violence. The "threats to the security of Canada," which it is specifically charged to investigate, include "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state . . ." [section 2(c), *CSIS Act*].

In addition to informing the Government in general about the nature of security threats to Canada, CSIS' intelligence and advice is specifically directed at several government departments or agencies. The information can form the basis for immigration screening profiles used in processing immigrants. In specific cases, CSIS advice can play an instrumental role in determining the admissibility of an applicant, or in denying citizenship. Security intelligence may also serve as a basis for determining an individual's suitability to have access to classified information, as well as assisting the police in crime prevention and in criminal prosecutions.

COUNTER TERRORISM

The role of the Counter Terrorism (CT) Branch is to advise the government on emerging threats of serious violence that could affect the safety and security of Canadians and of Canada's allies. Whether of domestic or foreign origin, addressing the threat of serious politically motivated violence continues to be one of the Service's chief priorities.

During 2000–2001, CT Branch made organizational and structural changes to reflect the evolving nature of the terrorist threat. The Service believes that one of the major challenges facing its counter terrorist efforts is the increasing use by extremists of advanced technologies to conduct, support and mask their operations.

Threat Assessments

CSIS provides threat assessments to departments and agencies within the federal government based on relevant and timely intelligence. CSIS prepares these assessments—dealing with special events, threats to diplomatic establishments in Canada and other situations—either upon request or unsolicited. Threat assessments can play a crucial role, not only in advising authorities when an activity such as a demonstration is likely to degenerate into violence, but also in reassuring authorities about situations in which there is little likelihood of violence.

In 2000–2001, the Threat Assessment Unit produced 544 assessments—a slight increase over the previous year. The Committee recognizes that many factors influencing this total—the number of foreign visitors to Canada, requests received from other government departments and agencies, special events and new threats identified during the year—are beyond the control of the Service.

REQUIREMENTS, ANALYSIS AND PRODUCTION

The research arm of CSIS, the Requirements, Analysis and Production (RAP) Branch provides advice to the Government on the threats to the security of Canada through the production of *CSIS Reports*, *CSIS Studies* and *CSIS Intelligence Briefs*. Using open source material, the Branch also produces two unclassified reports of security interest to both the intelligence community and the public, *Perspectives* and *Commentary*.

In 2000–2001, RAP produced 93 reports, almost double the number of the previous year and a significant reversal of the trend in recent years to issuing fewer reports. RAP publications generally fall under two categories:

- public safety reports examine the threat to Canadians at home and abroad from international terrorism;

- national security reports refer to the activities in Canada of other national governments' intelligence services, and global issues such as counter-proliferation and transnational criminal activities.

CSIS also contributes to the wider government intelligence community by participating in the Intelligence Assessment Committee (IAC). This body is made up of senior officials from departments and agencies of the Government of Canada most concerned with intelligence matters. In the year under review, RAP staff contributed to eight of the IAC's reports; these are distributed to a senior readership across government.

In an earlier report (*SIRC Report 1998–1999*), the Committee recommended reinvigorating the Executive Intelligence Production Committee (EXIPC), an internal CSIS body first set up in 1987 (but which had fallen into disuse) to help ensure that the intelligence produced conformed to the needs of the Service's various government clients. The Service has since decided to discard the annual planning cycle it originally envisaged for EXIPC in favour of more frequent monitoring of RAP's intelligence production activities with appropriate accountability to relevant senior Service managers. In future, formal meetings of EXIPC will be convened only as required.

Arrangements with Other Departments and Governments

RELATIONS WITH THE RCMP

The mechanisms to facilitate liaison and co-operation between CSIS and the RCMP are set out in the Memorandum of Understanding (MOU) between the two agencies. Co-operation is facilitated by the reciprocal assignment of liaison officers to the agencies' national headquarters and to all regional offices.

For the year under review, the Service cited several new initiatives aimed at improving co-operation with the Force:

- a staff exchange program between national headquarters with special emphasis on transnational criminal activity;
- exchanges of staff and agreements for future exchanges between several regional offices;
- "open houses" conducted by CSIS for the RCMP and other police forces at the regional level.

CSIS and the RCMP routinely exchange information about their activities pursuant to their respective mandates. The Service collects and disseminates information about threats to the security of Canada and the RCMP carries out its mandated law enforcement functions in relation to the same threats. During fiscal year 2000–2001, the two organizations exchanged 1678 documents, with CSIS responsible for generating more than half of the total (949). The Service also provided the RCMP with 330 disclosure letters[4] and 39 advisory letters.[5]

DOMESTIC ARRANGEMENTS

In carrying out its mandate, CSIS co-operates with police forces, and with federal and provincial departments and agencies across Canada. Contingent on Ministerial approval, the Service may conclude written co-operation arrangements with domestic agencies pursuant to section 17(1)(a) of the *CSIS Act*.

Currently, CSIS has 19 formal Memoranda of Understanding (MOUs) with federal government departments and agencies, and 8 with provincial bodies. The Service has a separate MOU with several police forces based in one province.

In 2000–2001, the Service signed a new arrangement with a provincial agency to conduct security assessments and sought Ministerial approval to establish a liaison arrangement with another. No existing arrangements were altered or terminated.

FOREIGN ARRANGEMENTS

Pursuant to section 17(1)(b) of the *CSIS Act*, the Service must obtain the approval of the Solicitor General—after consulting with the Minister of Foreign Affairs and International Trade—to enter into an arrangement with the government of a foreign state or an international organization. During the initial phases leading to the approval of an arrangement, CSIS is not permitted to pass classified information to the foreign agency; it may, however, accept unsolicited information.

During fiscal year 2000–2001, CSIS received the Minister's approval to establish five new liaison arrangements. Of the arrangements currently in force, the Service

---

4. Following a formal request by the RCMP, CSIS discloses information in a format that protects the identity of sources and the methods of intelligence gathering. The disclosure is made on the condition that the information can only be used for investigative leads and cannot be used in judicial proceedings.

5. Following a formal request by the RCMP—usually subsequent to a disclosure—CSIS gives permission in the form of an advisory letter for its information to be used in judicial proceedings, for example in obtaining warrants or as evidence at trial.

considers 44 to be "dormant."[6] Six existing arrangements were expanded to broaden the scope of information to be shared and one dormant arrangement was reactivated to facilitate Service security screening and immigration activities in the country concerned.

No existing liaison arrangements were cancelled; however, the Service curtailed the level of exchange activity with two foreign agencies, in one case because of human rights concerns and, in the other, because of an assessment that raised questions about that agency's reliability and stability.

SERVICE LIAISON OFFICER POSTS

The Service operates Security Liaison Officer (SLO) posts overseas responsible for liaising with police, security and intelligence agencies in many countries. The authorities in the host countries are aware of the Service officer's presence and functions, a necessary pre-condition for inter-agency co-operation. The number of SLO posts abroad was unchanged from the previous year.

Foreign intelligence refers to information or intelligence about the capabilities, intentions or activities of a foreign state

Collection of Foreign Intelligence

Under section 16 of the *CSIS Act*, the Service—at the written request of the Minister of Foreign Affairs and International Trade (DFAIT) or the Minister of National Defence (DND), and with the written consent of the Solicitor General—may collect foreign intelligence. Under the Act, CSIS can make warrant applications for powers such as telephone intercepts and undertake other investigative activities at the request of these ministers.

Foreign intelligence refers to information or intelligence about the "capabilities, intentions or activities" of a foreign state. The *CSIS Act* stipulates that the Service's collection of foreign intelligence must take place in Canada and cannot be directed at citizens of Canada, permanent residents or Canadian companies.

---

6. A dormant arrangement is one in which there has been no contact for 1 year or more. Liaison arrangements become dormant for a number of reasons: a simple lack of need to exchange information, concerns by the Service about the other agency's professional or human rights practices, or an assessment that the political situation in the other country is too unstable.

METHODOLOGY OF THE AUDIT

The Committee's review encompasses all Ministerial requests for assistance, all information about Canadians retained by CSIS for national security purposes and all exchanges of information with the Communications Security Establishment (CSE) in the context of foreign intelligence.

CSE—an agency of the Department of National Defence—provides the Government of Canada with foreign signals intelligence, which it obtains by gathering and analyzing foreign radio, radar and other electronic emissions, sometimes in co-operation with allied agencies.

The goal of the audit is to:

- review CSIS involvement in section 16 requests so as to ensure compliance with the *CSIS Act*, directions from the Federal Court and the governing 1987 Memorandum of Understanding (MOU) between the Ministers of Foreign Affairs and International Trade, National Defence and the Solicitor General;
- determine whether the Service has met the various legal conditions necessary to collect information under section 16 operations;
- examine the nature of the Service's co-operation with CSE to ensure that it is appropriate and complies with the law.

FINDINGS OF THE COMMITTEE

Warrant Implementation

As in any intelligence collection activity that involves a Federal Court warrant, the Service is obligated to observe all conditions and restrictions contained therein. The Committee examined a selection of warrants directed at section 16 collection as well as the associated affidavits and working files. In the cases we reviewed, the warrants were correctly administered and the relevant conditions observed.

Information Requests to the CSE

Information that CSE gives to the Service is routinely "minimized" to comply with the prohibition against targeting Canadian nationals and Canadian businesses. Thus, the name of a Canadian, which had been collected incidentally, would be shielded by employing, for example, the phrase "a Canadian business person." Under specific circumstances, the Service may request the identities from CSE if it can demonstrate that the information relates to activities which could constitute a threat to the security of Canada as defined in section 2 of the *CSIS Act*.

As part of its audit, the Committee scrutinized these CSIS requests to ensure that they were appropriate, and in accordance with law and policy; three did not appear to meet the threshold set out in section 2 of the Act.

One request involved a prominent Canadian who had been approached by a foreign national. The second request concerned a sensitive institution (trade union, media organization, religious body or university campus) involved in political campaigns in a foreign country. We were informed by the Service that in both instances the information obtained was removed from its files following our review.

In the third request, the Service had retained in its files lists of individuals who had attended several social functions with foreign nationals. Records checks were conducted by CSIS on some of the individuals listed.

The Committee questioned the retention of this information, citing to the Service our view that the action did not appear to meet the "strictly necessary" test of the Act. The Service maintained that the information was retained because the individuals had relationships with a target who was already the subject of a section 12 investigation. The Committee was satisfied with the Service's response.

Section 2

Security Screening and Investigation of Complaints

Security Screening and Investigation of Complaints

The Committee has a dual mandate under the *CSIS Act*: to review all CSIS activities and to investigate complaints about those activities. This section of the report deals with the second of the Committee's main responsibilities. In addition, since some of the complaints received arise out of the Service's security screening functions, our review of this part of the Service's mandate provides appropriate background and context for the subsequent discussion of complaints.

A. Security Screening

The Service has the authority, under section 13(1) of the *CSIS Act*, to provide security assessments to federal government departments. In addition, the Service may, with appropriate Ministerial approval, enter into arrangements to provide assessments to provincial government departments or provincial police forces, as outlined in section 13(2). Arrangements for the provision of security screening advice to foreign governments, foreign agencies and international institutions and organizations are authorized under section 13(3).

For federal employment, CSIS security assessments serve as the basis for determining whether an individual should be granted access to classified information or assets. In immigration cases, Service assessments can be instrumental in Citizenship and Immigration Canada's decision to admit an individual into the country and in granting permanent resident status or citizenship.

SECURITY SCREENING FOR FEDERAL EMPLOYMENT

2000–2001 Key Statistics

- The Service received 36 803 requests for security screening assessments for clearances, levels one through three, new, upgraded and updated. A preponderance of the total were for Level II clearances. In addition, 418 requests were for action relating to administrative procedures, such as transfers and downgrades.

- The average time required to complete a Level I security assessment was 32 days; for Level II, 41 days; and for Level III, 113 days.

Security Screening in the Government of Canada

The Government Security Policy (GSP) stipulates two types of personnel screening: a reliability assessment and a security assessment. Reliability checks and security assessments are conditions of employment under the *Public Service Employment Act*.

Basic Reliability Status

Every department and agency of the federal government has the responsibility to decide the type of personnel screening it requires. These decisions are based on the sensitivity of the information and the nature of the assets to which access is sought. Reliability screening at the "minimum" level is required for those persons who are appointed or assigned to a position for six months or more in the Public Service, or for those persons who are under contract with the federal government for more than six months, and who have regular access to government premises. Those persons who are granted reliability status at the basic level are permitted access to only non-sensitive information (i.e., information that is not classified or designated).

Enhanced Reliability Status

Enhanced Reliability Status is required when the duties of a federal government position or contract require the person to have access to classified information or government assets, regardless of the duration of the assignment. Persons granted enhanced reliability status can access the designated information and assets on a "need-to-know" basis.

The federal departments and agencies are responsible for determining what checks are sufficient in regard to personal data, educational and professional qualifications and employment history. Departments can also decide to conduct a criminal records name check (CRNC).

When conducting the reliability assessments, the federal government organizations are expected to make fair and objective evaluations that respect the rights of the individual. The GSP specifies that "individuals must be given an opportunity to explain adverse information before a decision is reached. Unless the information is exemptible under the *Privacy Act*, individuals must be given the reasons why they have been denied reliability status."

Security Assessments

The *CSIS Act* defines a security assessment as an appraisal of a person's loyalty to Canada and, so far as it relates thereto, the reliability of that individual. A "basic" or "enhanced" reliability status must be authorized by the government department or agency prior to requesting a security assessment. Even if a person has been administratively granted the reliability status, that individual must not be appointed to a position that requires access to classified information and assets, until the security clearance has been completed.

- Of the 3670 field investigations conducted, the largest number was for the Department of National Defence, followed by CSIS, the Department of Foreign Affairs and International Trade, the Communications Security Establishment and the Department of Public Works and Government Services.

- The Service received 37 128 requests for assessments under the Airport Restricted Access Area Clearance Program (ARAACP), which is under the authority of Transport Canada. The average turnaround time for a request under ARAACP was 32 days, a significant increase from last year's figure of 4 days. The Service attributed the difference to the volume of security screening requests and the resulting backlog of cases waiting to be processed.

- There were 1439 requests for security assessments related to "site access." These involve basic checks to provide clearances allowing an individual access to sensitive sites.

- With the RCMP acting as intermediary, the Service received 268 requests for accreditation to access the Parliamentary Precinct and 11 129 requests for accreditation to special events and functions to which access is controlled.

IMMIGRATION SECURITY SCREENING PROGRAMS

Under the authority of sections 14 and 15 of the *CSIS Act*, the Service conducts security screening investigations and provides advice to the Minister of Citizenship and Immigration Canada (CIC). Generally speaking, the Service's assistance takes the form of information- sharing on matters concerning threats to the security of Canada as defined in section 2 of the *CSIS Act* and the form of "assessments" with respect to the inadmissibility classes of section 19 of the *Immigration Act*.

Applications for Permanent Residence from Within Canada

The Service has the sole responsibility for screening immigrants and refugees who apply for permanent residence status from within Canada. In 2000–2001, the Service received 44 278 such screening requests.[7] The median turnaround time for screening applications was 66 days—with an average of 60 days to process electronic applications and 195 days for paper applications.

7. This number includes 4217 requests for security screening of applications originating in the USA and processed in Canada.

Applications for Permanent Residence from Outside Canada

Immigration and refugee applications for permanent residence that originate outside Canada or the USA are managed by the Overseas Immigrant Screening Program under which the Service shares responsibility for security screening with CIC officials based abroad. Generally, CSIS only becomes involved in the screening process if requested to do so by the Immigration Program Manager (IPM) or upon receiving adverse information about a case from established sources. This division of labour allows the Service to concentrate on the higher risk cases.

In 2000–2001, the Service received 25 109 requests to screen overseas applicants. Of these, CSIS reported that 4433 applicant files were referred by IPMs to CSIS Security Liaison Officers (SLOs) for consultation from April 1 to December 31, 2000.

Nature of the Service's Advice to CIC

Requests for security screening in relation to immigration resulted in 216 CSIS briefs to CIC—167 inadmissible briefs and 49 information briefs. During the period under review, the average time taken for the Service to process a case involving a brief was about a year and a half. The Service sent 90 "incidental letters" to CIC and 61 update letters. (*See* page 12 for a description of the Service's security screening briefs and other information-sharing mechanisms employed in aid of Canada's immigration programs.)

The times taken by CSIS to process requests from CIC rose significantly over those of previous years

Security Screening: Increased Turnaround Times

Overall, the times taken by CSIS to process requests from CIC rose significantly over those of previous years. The Service cited two main causes for the increased delays, both of which it regards as temporary. There had accumulated a significant number of overseas, "hard copy" cases, which take significantly longer to process than the Canada-based electronic cases. CSIS assured the Committee that it has eliminated this backlog and taken steps to prevent future backlogs. In addition, problems during the year in implementing new software combined with the necessary adjustments for the Y2K problem created further delays. The software difficulties are in the process of being resolved.

Citizenship Applications and the Watch List

As part of the citizenship application process, the Service receives electronic trace requests from CIC's Case Processing Centre in Sydney, Nova Scotia. The names of

citizenship applicants are cross-checked against the names in the Security Screening Information System database. The Service maintains a Watch List, which is made up of individuals who have come to the attention of CSIS through, *inter alia*, TARC-approved investigations and have received landed immigrant status.

In 2000–2001, the Service reviewed 161 895 citizenship applications. CSIS recommended that citizenship be denied in four instances and prepared information briefs in relation to 78 others. In one case, the Service sought Ministerial approval to defer its advice.[8]

A New Program: Refugee Screening

As discussed in the Committee's review of immigration security screening briefs (*see* page 12) the Service and CIC have recently concluded an agreement to conduct "Front-End Screening" of refugee applicants. Starting as a pilot project, facilities for exchanging electronic information are to be installed at five CIC sites across Canada.

SCREENING ON BEHALF OF FOREIGN AGENCIES

The Service may enter into reciprocal arrangements with foreign agencies to provide security checks on Canadians and other individuals who have resided in Canada. In the period under review, the Service concluded 995 foreign screening checks, 66 of which required field investigations. These investigations resulted in one information brief to the client.

B. Investigations of Complaints

In addition to the Committee's audit and review functions, we have the added responsibility to investigate complaints from the public about any CSIS action. Three kinds of complaints come within the Committee's purview:

1) Acting as a quasi-judicial tribunal, the Committee is empowered to consider and report on any matter having to do with federal security clearances, including complaints about denials of clearances to government employees and to contractors.

8. When the Service believes that it is not in a position to render a recommendation to CIC concerning a citizenship application, it must seek approval from the Solicitor General to continue investigating the case and "defer" providing the assessment.

2) The Committee can investigate reports made by federal ministers about persons in relation to citizenship and immigration, certain human rights matters and organized crime.

3) As stipulated in the *CSIS Act*, the Committee can receive at any time a complaint lodged by a person "with respect to any act or thing done by the Service."

FINDINGS ON SECTION 41 COMPLAINTS RE: "ANY ACT OR THING"

During the 2000–2001 fiscal year, the Committee dealt with 69 complaints made in relation to section 41 of the *CSIS Act*. Of these, 52 were new complaints and 17 were cases carried forward from the previous fiscal year (see Table 2).

Complaints Related to Immigration Matters

Continuing a pattern set in recent years, many of the complaints conveyed to the Committee in 2000–2001 related to the Service's role in Canada's immigration program—34 cases in all.

Complaints Concerning Improper Conduct and Abuse of Power

The Committee dealt with 20 complaints in the period under review from persons who alleged that the Service had subjected them to surveillance, illegal actions or had otherwise abused its powers.

So as not to confirm indirectly which targets are of interest to the Service, the Committee does not as a rule confirm or deny if a complainant is the subject of a

Table 2
Complaints (April 1, 2000 to March 31, 2001)

2) The Committee can investigate reports made by federal ministers about persons in relation to citizenship and immigration, certain human rights matters and organized crime.

3) As stipulated in the *CSIS Act*, the Committee can receive at any time a complaint lodged by a person "with respect to any act or thing done by the Service."

FINDINGS ON SECTION 41 COMPLAINTS RE: "ANY ACT OR THING"

During the 2000–2001 fiscal year, the Committee dealt with 69 complaints made in relation to section 41 of the *CSIS Act*. Of these, 52 were new complaints and 17 were cases carried forward from the previous fiscal year (*see* Table 2).

Complaints Related to Immigration Matters

Continuing a pattern set in recent years, many of the complaints conveyed to the Committee in 2000–2001 related to the Service's role in Canada's immigration program—34 cases in all.

Complaints Concerning Improper Conduct and Abuse of Power

The Committee dealt with 20 complaints in the period under review from persons who alleged that the Service had subjected them to surveillance, illegal actions or had otherwise abused its powers.

So as not to confirm indirectly which targets are of interest to the Service, the Committee does not as a rule confirm or deny if a complainant is the subject of a

CSIS targeting authority. Although this information is not provided to complainants, the Committee thoroughly investigates the complainant's allegations.

Through its investigations, the Committee assures itself that the Service's activities have been carried out in accordance with the Act, Ministerial Direction and CSIS policy. If we find that the Service has acted appropriately, we convey that assurance to the complainant. If the Committee identifies issues of concern, we share those with the Director of CSIS and the Solicitor General, and to the extent possible, report on the matter in our annual report.

During 2000–2001, most of the Committee's investigations into this type of complaint revealed that the Service was neither involved in, nor responsible for, the activities alleged by the complainant.

Complaints the Committee is Precluded from Investigating

The Committee received 26 complaints that it was precluded from investigating because the criterion set out in section 41 of the Act, which requires that complaints first be sent to the Director of CSIS, had not been met. The Committee responds to such complaints by outlining the requirements of section 41 and providing the address to communicate with the Director. The Committee is also precluded from investigating complaints in which complainants are entitled to seek redress through a grievance procedure established under the *CSIS Act* or the *Public Service Staff Relations Act*.

Misdirected Complaints

The Committee received 12 complaints that either did not involve the Service or were not related to matters of national security. In such cases, the Committee informs the individual that the complaint is not within our jurisdiction and, if possible, redirects the complainant to the appropriate authorities.

SECURITY CLEARANCE COMPLAINTS

The Committee dealt with four complaints under section 42 of the Act relating to security clearances in 2000–2001. Two cases, involving the revocation of security clearances, were completed; in one instance the complaint was withdrawn and, in the other, the Committee investigated and reached a decision, which is summarized in Appendix D. The other two complaints concerned Service recommendations to deny security clearances; the Committee's inquiries into these complaints continue.

FINDINGS ON MINISTERIAL REPORTS

Citizenship Refusals

In the ongoing matter of the citizenship application of Ernst Zündel—a matter first brought before the Committee in 1995—we were notified in December 2000 that Mr. Zündel was withdrawing his application for Canadian citizenship, and that this withdrawal had been accepted by Citizenship and Immigration Canada. In light of this information, there was no basis for continuing to investigate the matter. The Committee will not, therefore, issue a report on the matter to the Governor in Council pursuant to section 19(6) of the *Citizenship Act*.

Reports Pursuant to the *Immigration Act*

The Committee received no such Ministerial Reports during the period under review. As discussed in last year's Report, a case relating to a SIRC decision issued in 1998 (Yamani) was referred back to the Committee in March 2000 for reconsideration. The Committee has since been advised that Citizenship and Immigration Canada has decided not to pursue the matter. As a result, the case is no longer before the Committee.

CANADIAN HUMAN RIGHTS COMMISSION REFERRAL

The Committee received no Human Rights Commission referrals in the period under review. However, the investigation of a referral received last year was completed and reported to the Commission.

Section 3

CSIS Accountability Structure

CSIS Accountability Structure

The Service is an agency of the Government of Canada and through the Solicitor General is accountable to Parliament and to the people of Canada. Because of the serious and potentially intrusive nature of CSIS activities, the mechanisms set out in law to give effect to that accountability are both rigorous and multi-dimensional; a number of independently managed systems exist inside and outside the Service for monitoring CSIS activities and ensuring that they are conducted in a manner consistent with its mandate and the law.

A full description of Canada's security intelligence apparatus and the accompanying accountability mechanisms can be found in a new publication of the Privy Council Office, *The Canadian Security and Intelligence Community*, Ottawa, 2001.

Part of SIRC's task—the Committee itself being part of the accountability structure—is to assess and comment on the functioning of the systems that hold the Service responsible to its Minister.

A. Operation of CSIS Accountability Mechanisms

MINISTERIAL DIRECTION

Under section 6(2) of the *CSIS Act*, the Minister can issue directions governing CSIS activities and investigations. The Committee is specifically charged with reviewing those directions when they are issued. In fiscal year 2000–2001, the Minister issued a new compendium of Ministerial Direction, which replaces the previous documents in their entirety. The subject of a special Committee review, the revised and updated Direction is discussed in greater detail on page 7.

CHANGES IN SERVICE OPERATIONAL POLICIES

In the fiscal year 2000–2001, the Service produced two new policies: one deals with preparing threat assessments, and the other with using the polygraph in CSIS operations. Another 14 policies were amended either to reflect changes in Ministerial Direction or to conform with current business practice.

DISCLOSURES IN THE PUBLIC INTEREST AND IN THE NATIONAL INTEREST

Section 19 of the *CSIS Act* prohibits information obtained by the Service in the course of its investigations from being disclosed except in specific circumstances. Under section 19(2)(d) the Minister can authorize the Service to disclose

information in the "public interest." The Act instructs the Director of CSIS to submit a report to the Committee regarding all public interest disclosures.

The Service reported one such disclosure in 2000–2001. The disclosure was to counsel acting on behalf of a Minister of the Crown and related to a Service employee's draft affidavit prepared in relation to legal proceedings.

In addition, CSIS acting as the Minister's agent can disclose information in the "national interest" under specified circumstances. Service policy stipulates that the Committee must be informed when such disclosures occur. There were none during the year under review.

GOVERNOR IN COUNCIL REGULATIONS AND APPOINTMENTS

As set out in section 8(4) of the *CSIS Act*, the Governor in Council may issue any regulations to the Service in regard to the powers and duties of the Director of CSIS, as well as the conduct and discipline of Service employees. No such regulations were issued in fiscal year 2000–2001.

CERTIFICATE OF THE INSPECTOR GENERAL

The Inspector General of CSIS reports to the Solicitor General and functions effectively as the Minister's internal auditor of CSIS, reviewing the operational activities of the Service and monitoring compliance with policy and the law. Every year the Inspector General must submit to the Minister a Certificate stating the "extent to which [he or she] is satisfied" with the Director's annual report on the operational activities of the Service, and informing the Minister of any instances of CSIS having failed to comply with the Act or Ministerial Direction, or which involved an unreasonable or unnecessary exercise of powers. The Minister forwards the Certificate to the Review Committee.

The first certificate from the current Inspector General, who was appointed in July 1999, was issued in November 2000. In it, the Inspector General stated that he was fully satisfied with the Director's annual report to the Minister and that in his opinion, "the Service ha[d] not acted beyond the framework of its statutory authority, ha[d] not contravened any Ministerial Directions, and ha[d] not exercised its powers unreasonably or unnecessarily."

The Inspector General went on to state that he and the Director of CSIS had come to an agreement that future Director's reports would be more concise and focussed than hitherto. Future reports would present "the highlights of the Service's activities for the reporting period, and include any serious issues with respect to operational activities, public policy, potential controversy, and anticipated challenges in fulfilling the Service's mandate." Supplementary detailed data would continue to be available

for examination by the Deputy Solicitor General, the Inspector General's Office and this Committee.

The other matter addressed by the Inspector General concerned a security certificate signed by the Minister of Citizenship and Immigration and the Solicitor General based on a security intelligence report prepared by the Service. A subsequent Federal Court ruling quashed the certificate, judging it to be "not reasonable."

The Inspector General conducted his own assessment of the CSIS security intelligence report and concluded that it was well founded, accurate and credible, and that it met the "reasonable grounds to believe" standard set out in section 19(1) of the *Immigration Act*. He also stated that he supported measures underway within the Service that would result in security intelligence reports that in future were "more cogent and compelling when presented to the Court."

UNLAWFUL CONDUCT

Under section 20(2) of the *CSIS Act*, the Director of CSIS is to submit a report to the Minister when, in his opinion, a CSIS employee may have acted unlawfully in performing his or her duties and functions. The Minister, in turn, must send the report with his comment to the Attorney General of Canada and to the Committee.

In 2000–2001, we received one report of possible unlawful conduct by an employee of CSIS. At the time of publication of this Report, the Attorney General has not yet rendered a decision as to the disposition of the case. In last year's Report (*SIRC Report 1999–2000*), we cited an unresolved case of unlawful conduct dating back to 1997. The Attorney General has since decided not to proceed with prosecution.

SECTION 2(D) INVESTIGATIONS

According to Ministerial Direction, any investigation of threats to the security of Canada as defined by section 2(d) of the *CSIS Act*—often referred to as the "subversion" clause—must be authorized by the Minister. The Minister authorized no such investigations in 2000–2001.

B. Inside the Security Intelligence Review Committee

TRACKING AND TIMING OF FORMAL INQUIRIES

In carrying out its review function the Committee sends questions to CSIS to request information or documents (or both) about its activities. In fiscal year 2000–2001

(April 1, 2000 to March 31, 2001), we directed 91 formal inquiries to the Service, which total does not include inquiries arising from complaints cases.

The Committee often makes additional informal requests of CSIS. During the year under review, the Service responded expeditiously to what were sometimes urgent inquiries.

RESEARCH AND REVIEW ACTIVITIES

The Service makes available a separate office and computers at CSIS Headquarters for the exclusive use of SIRC staff and members. Reporting regularly to the Committee's senior management, SIRC's researchers and analysts divide their time between SIRC premises and the Committee's facilities at the Service.

BRIEFINGS

At its monthly meetings, the Chair and Committee Members meet with government officials to keep the lines of communications open and stay abreast of new developments. When meetings of the Committee are held outside Ottawa, Members visit CSIS regional offices. In June 2000 and February 2001, the Committee met with senior CSIS regional managers in Toronto and, in September 2000, with Service officials in Montréal. The balance of the meetings were held in Ottawa.

SENIOR STAFF APPOINTMENTS AT SIRC

In December 2000, Susan Pollak, Executive Director of SIRC, announced the appointment of Mr. Thomas Dastous as the Senior Counsel to SIRC. Mr. Dastous joined SIRC from the federal Department of Justice.

In January 2001, Ms. Kelly McGee joined SIRC as Research Manager. Previously, Ms. McGee was Senior Counsel and Director of Policy at the Regional Municipality of Ottawa–Carleton.

ADDITIONAL COMMITTEE ACTIVITIES

- In September 2000, the Chair, Executive Director, Deputy Executive Director and Senior Counsel met in Ottawa with the recently appointed Inspector-General of Intelligence for South Africa to discuss the role and functions of the Security Intelligence Review Committee in Canada's system of government.

- A delegation from Denmark met with SIRC senior management in October 2000 to discuss the Committee's mandate and operations. The delegation was conducting research as part of a commission examining Denmark's intelligence services.

- The National Security Advisor to Mexican President Vicente Fox met with the Executive Director, Deputy Executive Director and Senior Counsel in February 2001 to discuss SIRC's mandate, structure and operations, and to share some of its experiences over the past 16 years.

- In March 2001, members of the Norwegian Committee for the Monitoring of Intelligence, Surveillance and Security met with SIRC senior management as part of the group's study tour in North America. The Norwegian Committee viewed the SIRC model as being of special interest in its survey of similar bodies.

ON THE INTERNET

In fiscal 2000–2001, SIRC's Web site underwent major reconstruction to present a more attractive, more user-friendly source of information for Canadians. All SIRC Annual Reports, dating back to its establishment in 1984, are accessible through the redesigned site at *www.sirc-csars.gc.ca*. The site presents the latest news about Committee activities, as well as information ranging from biographical information on Committee Members to procedures for filing complaints about CSIS activities and the denial of security clearances. During the 2000–2001 reporting period, the site recorded 543 137 hits; some 45 000 per month or approximately 1500 per day.

BUDGET AND EXPENDITURES

The Committee continues to manage its activities within the resource levels established in 1985. During 2000–2001, the Committee continued to deal with an increase in the number of quasi-judicial (complaint) proceedings with a concomitant effect on the Committee's non-discretionary expenditures (*see* Table 3).

- The National Security Advisor to Mexican President Vicente Fox met with the Executive Director, Deputy Executive Director and Senior Counsel in February 2001 to discuss SIRC's mandate, structure and operations, and to share some of its experiences over the past 16 years.

- In March 2001, members of the Norwegian Committee for the Monitoring of Intelligence, Surveillance and Security met with SIRC senior management as part of the group's study tour in North America. The Norwegian Committee viewed the SIRC model as being of special interest in its survey of similar bodies.

ON THE INTERNET

In fiscal 2000–2001, SIRC's Web site underwent major reconstruction to present a more attractive, more user-friendly source of information for Canadians. All SIRC Annual Reports, dating back to its establishment in 1984, are accessible through the redesigned site at *www.sirc-csars.gc.ca*. The site presents the latest news about Committee activities, as well as information ranging from biographical information on Committee Members to procedures for filing complaints about CSIS activities and the denial of security clearances. During the 2000–2001 reporting period, the site recorded 543 137 hits: some 45 000 per month or approximately 1500 per day.

BUDGET AND EXPENDITURES

The Committee continues to manage its activities within the resource levels established in 1985. During 2000–2001, the Committee continued to deal with an increase in the number of quasi-judicial (complaint) proceedings with a concomitant effect on the Committee's non-discretionary expenditures (see Table 3).

Table 3
SIRC Expenditures

	[illegible]	[illegible]	[illegible]
Personnel	[illegible]	[illegible]	[illegible]
Goods and Services	[illegible]	[illegible]	[illegible]
Total	[illegible]	[illegible]	[illegible]

Other significant expenses included:

- upgrades to the in-house computer infrastructure to be able to meet current operational and security standards for handling large volumes of highly classified information;
- upgrades to the simultaneous translation system in the Committee hearing room;
- improvements to the public access areas and hearing rooms, aimed at creating a more welcoming and, at the same time, more functional environment;
- travel expenses within Canada for Committee hearings and Research staff audit activity;
- staff salaries and benefits.

STAFFING AND ORGANIZATION

The Committee has a staff of 16: an Executive Director, a Deputy Executive Director, a Senior Counsel, a Junior Counsel, one Complaints/Access to Information and Privacy Officer, a Senior Para-legal/Hearing Registrar, a Research Manager, a Senior Policy Advisor, four Research Analysts, a Financial/Office Administrator, an Administrative Assistant, and two administrative support staff to handle sensitive and highly classified material using special security procedures.

At their monthly meetings, Members of the Committee decide formally on the research and other activities they wish to pursue and set priorities for staff. Management of day-to-day operations is delegated to the Executive Director with direction, when necessary, from the Chair in her role as Chief Executive Officer.

Appendix A

Abbreviations

Abbreviations

ARAACP	Airport Restricted Access Area Clearance Program
CI	Counter Intelligence Branch
CIC	Citizenship and Immigration Canada
CPC	Case Processing Centre (CIC)
Committee	Security Intelligence Review Committee (SIRC)
CSE	Communications Security Establishment (DND)
CSIS	Canadian Security Intelligence Service
CT	Counter Terrorism Branch
DFAIT	Department of Foreign Affairs and International Trade
Director	The Director of CSIS
DND	Department of National Defence
EXIPC	Executive Intelligence Production Committee
GSP	Government Security Policy
IAC	Intelligence Assessment Committee (Privy Council Office)
IPM	Immigration Program Manager (CIC)
MOU	Memorandum of Understanding
NRT	No Reportable Trace
RAP	Requirements, Analysis and Production Branch

RCMP	Royal Canadian Mounted Police
RTA	Request for TARC Authority
Service	Canadian Security Intelligence Service (CSIS)
SIRC	Security Intelligence Review Committee
SLO	Security Liaison Officer
TARC	Target Approval and Review Committee

Appendix B

SIRC Reports and Studies Since 1984

SIRC Reports and Studies Since 1984

(Section 54 reports—special reports the Committee makes to the Minister—are indicated with an *)

1. *Eighteen Months After Separation: An Assessment of CSIS Approach to Staffing Training and Related Issues* (SECRET) * (86/87-01)

2. *Report on a Review of Security Screening for Applicants and Employees of the Federal Public Service* (SECRET) * (86/87-02)

3. *The Security and Intelligence Network in the Government of Canada: A Description* (SECRET) * (86/87-03)

4. *Ottawa Airport Security Alert* (SECRET) * (86/87-05)

5. *Report to the Solicitor General of Canada Concerning CSIS' Performance of its Functions* (SECRET) * (87/88-01)

6. *Closing the Gaps: Official Languages and Staff Relations in the CSIS* (UNCLASSIFIED)* (86/87-04)

7. *Counter-Subversion: SIRC Staff Report* (SECRET) (87/88-02)

8. *SIRC Report on Immigration Screening* (SECRET) * (87/88-03)

9. *Report to the Solicitor General of Canada on CSIS' Use of Its Investigative Powers with Respect to the Labour Movement* (PUBLIC VERSION) * (87/88-04)

10. *The Intelligence Assessment Branch: A SIRC Review of the Production Process* (SECRET)* (88/89-01)

11. *SIRC Review of the Counter-Terrorism Program in the CSIS* (TOP SECRET) * (88/89-02)

12. *Report to the Solicitor General of Canada on Protecting Scientific and Technological Assets in Canada: The Role of CSIS* (SECRET) * (89/90-02)

13. *SIRC Report on CSIS Activities Regarding the Canadian Peace Movement* (SECRET) * (89/90-03)

14. *A Review of CSIS Policy and Practices Relating to Unauthorized Disclosure of Classified Information* (SECRET) (89/90-04)

15. *Report to the Solicitor General of Canada on Citizenship/Third Party Information* (SECRET) * (89/90-05)

16. *Amending the CSIS Act: Proposals for the Special Committee of the House of Commons* (UNCLASSIFIED) (89/90-06)

17. *SIRC Report on the Innu Interview and the Native Extremism Investigation* (SECRET) * (89/90-07)

18. *Supplement to the Committee's Report on Immigration Screening of January 18, 1988* (SECRET) * (89/90-01)

19. *A Review of the Counter-Intelligence Program in the CSIS* (TOP SECRET) * (89/90-08)

20. *Domestic Exchanges of Information* (SECRET) * (90/91-03)

21. *Section 2(d) Targets—A SIRC Study of the Counter-Subversion Branch Residue* (SECRET) (90/91-06)

22. *Regional Studies (six studies relating to one region)* (TOP SECRET) (90/91-04)

23. *Study of CSIS' Policy Branch* (CONFIDENTIAL) (90/91-09)

24. *Investigations, Source Tasking and Information Reporting on 2(b) Targets* (TOP SECRET) (90/91-05)

25. *Release of Information to Foreign Agencies* (TOP SECRET) * (90/91-02)

26. *CSIS Activities Regarding Native Canadians—A SIRC Review* (SECRET) * (90/91-07)

27. *Security Investigations on University Campuses* (TOP SECRET) * (90/91-01)

28. *Report on Multiple Targeting* (SECRET) (90/91-08)

29. *Review of the Investigation of Bull, Space Research Corporation and Iraq* (SECRET) (91/92-01)

30. *Report on Al Mashat's Immigration to Canada* (SECRET) * (91/92-02)

31. *East Bloc Investigations* (TOP SECRET) (91/92-08)

32. *Review of CSIS Activities Regarding Sensitive Institutions* (TOP SECRET) (91/92-10)

33. *CSIS and the Association for New Canadians* (SECRET) (91/92-03)

34. *Exchange of Information and Intelligence between CSIS & CSE, Section 40* (TOP SECRET) * (91/92-04)

35. *Victor Ostrovsky* (TOP SECRET) (91/92-05)

36. *Report on Two Iraqis—Ministerial Certificate Case* (SECRET) (91/92-06)

37. *Threat Assessments, Section 40 Study* (SECRET) * (91/92-07)

38. *The Attack on the Iranian Embassy in Ottawa* (TOP SECRET) * (92/93-01)

39. *"STUDYNT" The Second CSIS Internal Security Case* (TOP SECRET) (91/92-15)

40. *Domestic Terrorism Targets—A SIRC Review* (TOP SECRET) * (90/91-13)

41. *CSIS Activities with respect to Citizenship Security Screening* (SECRET) (91/92-12)

42. *The Audit of Section 16 Investigations* (TOP SECRET) (91/92-18)

43. *CSIS Activities during the Gulf War: Community Interviews* (SECRET) (90/91-12)

44. *Review of CSIS Investigation of a Latin American Illegal* (TOP SECRET) * (90/91-10)

45. *CSIS Activities in regard to the Destruction of Air India Flight 182 on June 23, 1985—A SIRC Review* (TOP SECRET) * (91/92-14)

46. *Prairie Region—Report on Targeting Authorizations (Chapter 1)* (TOP SECRET) * (90/91-11)

47. *The Assault on Dr. Hassan Al-Turabi* (SECRET) (92/93-07)

48. *Domestic Exchanges of Information (A SIRC Review—1991/92)* (SECRET) (91/92-16)

49. *Prairie Region Audit* (TOP SECRET) (90/91-11)

50. *Sheik Rahman's Alleged Visit to Ottawa* (SECRET) (CT 93-06)

51. *Regional Audit* (TOP SECRET)

52. *A SIRC Review of CSIS' SLO Posts* (London & Paris) (SECRET) (91/92-11)

53. *The Asian Homeland Conflict* (SECRET) (CT 93-03)

54. *Intelligence-Source Confidentiality* (TOP SECRET) (CI 93-03)

55. *Domestic Investigations (1)* (SECRET) (CT 93-02)

56. *Domestic Investigations (2)* (TOP SECRET) (CT 93-04)

57. *Middle East Movements* (SECRET) (CT 93-01)

58. *A Review of CSIS SLO Posts* (1992-93) (SECRET) (CT 93-05)

59. *Review of Traditional CI Threats* (TOP SECRET) (CI 93-01)

60. *Protecting Science, Technology and Economic Interests* (SECRET) (CI 93-04)

61. *Domestic Exchanges of Information* (SECRET) (CI 93-05)

62. *Foreign Intelligence Service for Canada* (SECRET) (CI 93-06)

63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 93-11)

64. *Sources in Government* (TOP SECRET) (CI 93-09)

65. *Regional Audit* (TOP SECRET) (CI 93-02)

66. *The Proliferation Threat* (SECRET) (CT 93-07)

67. *The Heritage Front Affair. Report to the Solicitor General of Canada* (SECRET) * (CT 94-02)

68. *A Review of CSIS' SLO Posts (1993-94)* (SECRET) (CT 93-09)

69. *Domestic Exchanges of Information (A SIRC Review 1993–94)* (SECRET) (CI 93-08)

70. *The Proliferation Threat—Case Examination* (SECRET) (CT 94-04)

71. *Community Interviews* (SECRET) (CT 93-11)

72. *An Ongoing Counter-Intelligence Investigation* (TOP SECRET) * (CI 93-07)

73. *Potential for Political Violence in a Region* (SECRET) (CT 93-10)

74. *A SIRC Review of CSIS SLO Posts (1994–95)* (SECRET) (CT 95-01)

75. *Regional Audit* (TOP SECRET) (CI 93-10)

76. *Terrorism and a Foreign Government* (TOP SECRET) (CT 94-03)

77. *Visit of Boutros Boutros-Ghali to Canada* (SECRET) (CI 94-04)

78. *Review of Certain Foreign Intelligence Services* (TOP SECRET) (CI 94-02)

79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 94-01)

80. *Domestic Exchanges of Information (A SIRC Review 1994-95)* (SECRET) (CI 94-03)

81. *Alleged Interference in a Trial* (SECRET) (CT 95-04)

82. *CSIS and a "Walk-In"* (TOP SECRET) (CI 95-04)

83. *A Review of a CSIS Investigation Relating to a Foreign State* (TOP SECRET) (CI 95-02)

84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports* (TOP SECRET) (CI 95-05)

85. *Regional Audit* (TOP SECRET) (CT 95-02)

86. *A Review of Investigations of Emerging Threats* (TOP SECRET) (CI 95-03)

87. *Domestic Exchanges of Information* (SECRET) (CI 95-01)

88. *Homeland Conflict* (TOP SECRET) (CT 96-01)

89. *Regional Audit* (TOP SECRET) (CI 96-01)

90. *The Management of Human Sources* (TOP SECRET) (CI 96-03)

91. *Economic Espionage I* (SECRET) (CI 96-02)

92. *Economic Espionage II* (TOP SECRET) (CI 96-02)

93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996–97* (TOP SECRET) (CI 96-04)

94. *Urban Political Violence* (SECRET) (SIRC 1997-01)

95. *Domestic Exchanges of Information (1996–97)* (SECRET) (SIRC 1997-02)

96. *Foreign Conflict—Part I* (SECRET) (SIRC 1997-03)

97. *Regional Audit* (TOP SECRET) (SIRC 1997-04)

98. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1997-05)

99. *Spy Case* (TOP SECRET) (SIRC 1998-02)

100. *Domestic Investigations (3)* (TOP SECRET) (SIRC 1998-03)

101. *CSIS Cooperation with the RCMP—Part I* (SECRET) * (SIRC 1998-04)

102. *Source Review* (TOP SECRET) (SIRC 1998-05)

103. *Interagency Cooperation Case* (TOP SECRET) (SIRC 1998-06)

104. *A Case of Historical Interest* (TOP SECRET) (SIRC 1998-08)

105. *CSIS Role in Immigration Security Screening* (SECRET) (CT 95-06)

106. *Foreign Conflict—Part II* (TOP SECRET) (SIRC 1997-03)

107. *Review of Transnational Crime* (SECRET) (SIRC 1998-01)

108. *CSIS Cooperation with the RCMP—Part II* (SECRET) * (SIRC 1998-04)

109. *Audit of Section 16 Investigations & Foreign Intelligence 1997–98* (TOP SECRET) (SIRC 1998-07)

110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)

111. *Regional Audit* (TOP SECRET) (SIRC 1998-10)

112. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 1998-11)

113. *Allegations by a Former CSIS Employee* (TOP SECRET) * (SIRC 1998-12)

114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)

115. *Review of Foreign Intelligence Activities in Canada* (TOP SECRET) (SIRC 1998-15)

116. *Files* (TOP SECRET) (SIRC 1998-16)

117. *Audit of Section 16 Investigations & Foreign Intelligence* (TOP SECRET) (SIRC 1999-01)

118. *A Long-Running Counter Intelligence Investigation* (TOP SECRET) (SIRC 1999-02)

119. *Domestic Exchanges of Information* (TOP SECRET) (SIRC 1999-03)

120. *Proliferation* (TOP SECRET) (SIRC 1999-04)

121. *SIRC's Comments on the Draft Legislation Currently Before Parliament—Bill C-31* (PROTECTED) * (SIRC 1999-05)

122. *Domestic Targets* (TOP SECRET) (SIRC 1999-06)

123. *Terrorist Fundraising* (TOP SECRET) (SIRC 1999-07)

124. *Regional Audit* (TOP SECRET) (SIRC 1999-08)

125. *Foreign State Activities* (TOP SECRET) (SIRC 1999-09)

126. *Project Sidewinder* (TOP SECRET) (SIRC 1999-10)

127. *Security Breach* (TOP SECRET) (SIRC 1999-11)

128. *Domestic Exchanges of Information 1999–2000* (TOP SECRET) (SIRC 2000-01)

129. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1999–2000* (TOP SECRET) (SIRC 2000-02)

130. *CSIS Liaison with Foreign Agencies* (TOP SECRET) (SIRC 2000-03)

131. *Regional Audit* (TOP SECRET) (SIRC 2000-04)

132. *Warrant Review* (TOP SECRET) (SIRC 2000-05)

133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999–2000* (TOP SECRET) (SIRC 2001-02)

Appendix C

Major Findings and Recommendations

Major Findings and Recommendations

CSIS LIAISON WITH FOREIGN AGENCIES

The Committee audited a Security Liaison Officer (SLO) post overseas that operates in an especially difficult working environment. Maintaining the security of the physical operating environment is a major ongoing challenge. The situation is compounded by generally onerous working conditions. The Committee was struck by the substandard conditions in which Service staff were obliged to work. The poor physical facilities at Canada's mission, a heavy workload arising from increasingly large numbers of immigration and visa applications requiring security screening all combine to form an adverse environment. Notwithstanding these difficult circumstances, however, the SLO and staff are performing well.

We found that while the SLO has made steady progress with foreign interlocutors, rising demands from the immigration side of the SLO's mandate left less time for developing relationships with other countries in the region for which the post is nominally responsible.

The evident work overload gave rise to concerns on the part of the Committee that some of the post's important functions might not be being handled expeditiously. Service senior management told the Committee that it shared our concerns and believed that the immigration workload problem extended to certain other of its SLO posts as well. It is the Committee's view that the Service might wish to review this element of its Foreign Liaison Program.

The Committee examined all documentation associated with operational co-operation and information exchanges involving the SLO post from March 31, 1998 through June 30, 2000. Our review identified only one problematic exchange. We advised the Service that it should consider providing updated information to clients so that earlier advice is regarded in its proper context.

Concerns about potential impacts on human rights figured significantly in the Committee's audit of this particular post. SLOs are obligated to give the rest of the Service timely and accurate assessments of an agency's human rights record, and of its propensity to pass information on to third parties without authorization. With respect to the SLO post under review, the Committee identified no information exchanges that failed to conform to these standards and satisfied itself that all human rights assessments of agencies had been properly carried out.

MINISTERIAL DIRECTION, REVISED AND UPDATED

In February 2001, the Solicitor General issued a revised compendium of Ministerial Directions governing control and management of the Service—a development the Committee has looked forward to for some time.

The new compendium (a classified document) goes a long way to rationalizing the Government's strategic guidance of the Service and, in the Committee's view, reflects a maturation of the legal and policy framework that governs the Service's work. Ministerial guidance is now considerably streamlined, consistent in its use of language and presented in a concise and cohesive document. Also apparent is an overall shift in discretionary powers from the Office of the Solicitor General to the Director of CSIS, with respect to the day-to-day management of the Service. In the course of future audits, the Committee intends to pay particular attention to how the new guidance is interpreted and implemented across the range of CSIS activities.

DOMESTIC EXCHANGES OF INFORMATION (5)

The Committee examined all Service exchanges of information with other domestic agencies for the fiscal year 1999–2000. In addition, the Committee conducted an on-site review of information exchange practices in one Service regional office.

For the period under review, the Committee identified two exchanges that raised concern. In the first case, the Service's database holding the unsolicited material contained several items relating to individuals and organizations for which CSIS did not have targeting authorizations. We asked the Service to explain its reasons for retaining this material and were satisfied with the explanation. The Committee believes that in future, however, the rationale for retaining unsolicited information of a similar nature should be clearly set out in the relevant operational reports.

> **The Committee recommends that the purpose for retaining information under a general collection category be clearly identified in operational reports.**

The second case concerned the appropriateness of retaining certain information received from a domestic agency about the activities of a small group of minors. CSIS subsequently decided that no further action was needed but retained the original exchange of information in its files. It is the Committee's view that the information should be deleted from CSIS records. The Service did agree to modify

the operational reports to reflect the decision it ultimately made that the information warranted no further action on its part.

The Committee recommends that the Service employ greater diligence in deciding whether to retain unsolicited information.

SECURITY SCREENING BRIEFS TO CIC

The Committee examined a selection of the Service's immigration security screening investigations from the 166 briefs sent by CSIS to CIC in the 1999–2000 fiscal year. The Committee reviewed the briefs sent to CIC and all supporting documents relevant to each investigation. All the Service briefs to CIC in which the Service rendered an opinion were found to be accurate and adequately supported by the information collected.

The Committee has recently been advised that the Service and CIC have developed a "Front End Screening" program for refugee claimants in Canada. The aim of the program is to prevent persons from being able to enter Canada and remain for an indefinite period without undergoing a security screening assessment—a significant risk under the procedures in place at the time of a previous Committee review.

Appendix D

Complaint Case Histories

Complaint Case Histories

This appendix summarizes complaint cases submitted to the Review Committee during the past year on which decisions have been reached. Not addressed here are complaints that were handled through administrative review, were misdirected or were deemed to be outside the Committee's jurisdiction.

Where appropriate, complaints are investigated through a quasi-judicial hearing presided over by a Member of the Committee. After the hearings are complete, the presiding member renders a decision that is provided to the Solicitor General and the Director of CSIS. After any information with national security implications is removed, the complainant also receives a copy of the decision.

The Committee reported on two decisions reached during the period under review: one was a section 42 (denial of security clearance) matter and the other concerned a complaint lodged in accordance with section 41—"any act or thing."

CASE #1

The complainant was a former employee of the Service whose security clearance was revoked in 1999. As a result, the complainant was dismissed from the Service at which time the individual filed a complaint contesting the Service's denial of security clearance.

The Service's justification for revoking the clearance was based on the contention that the employee had failed to prevent classified information from being disclosed to the news media and, thus, had violated the professional oath taken by all Service employees. Since a security clearance was a prerequisite to being employed by the Service, dismissal followed immediately.

The complainant asserted that there was no justification for the Service's position in respect to the public disclosure. The complainant had contacted the news media to discuss a discrimination complaint against the Service. The complainant cast doubt on how thoroughly the Service investigated the matter and suggested, moreover, that the dismissal was carried out to hide errors made by the Service.

The Committee's investigation failed to find any information that supported the complainant's claims. The CSIS operation, which was the subject of the disclosure, was a legitimate activity undertaken in accordance with policy and the law.

Although the Service did make errors in managing the operation, this fact did not, in the Committee's view, absolve the employee of responsibility to protect classified information.

With regard to the Service's investigation of the unauthorized disclosure, our own inquiries showed that the Director's decision to revoke the security clearance was based on incomplete information. Nevertheless, the Committee found that the Director did have information sufficient to revoke the complainant's security clearance.

As the complainant's employment with the Service required a Level III clearance, the dismissal of the complainant subsequent to the revocation of the complainant's security clearance was inevitable. However, the Committee recommended that the Service facilitate the complainant's reassignment to another department of government, consistent with Government Security Policy. In addition, the Committee recommended that the Service reassess certain of its information management methods and procedures.

CASE #2

The complaint, lodged under section 41 of the *CSIS Act*, alleged that a particular Service operation had exposed the complainant to dangerous individuals, that a Service officer had behaved in a threatening and intimidating manner towards the complainant causing undue stress and anxiety and that the Service had ignored requests by the complainant for assistance. The complainant also made a claim for damages suffered as a result of lost income.

The Committee found no grounds to support the complainant's allegations. There was no evidence that the complainant had been put at risk by the Service, nor was there any evidence of malice or intimidation by the Service towards the complainant. The complainant admitted to the Committee that the Service officer had not in fact acted in a threatening or intimidating manner. The Committee also concluded that there was no basis for recommending the reimbursement of lost income.

Although the Committee found the complaint itself to be unfounded, we did note serious problems with the Service's supervision of the operation at issue. The Committee made a number of recommendations to the Service aimed at improving management and operating procedures in similar types of operations in the future.

COMITÉ DE SURVEILLANCE DES ACTIVITÉS
DE RENSEIGNEMENT DE SÉCURITÉ

Rapport du CSARS 2000–2001

Examen opérationnel du Service canadien du renseignement de sécurité

Canada

Comité de surveillance des activités de renseignement de sécurité
122, rue Bank
B.P. 2430, succursale D
Ottawa (Ontario)
K1P 5W5

Téléphone : (613) 990-8441
Télécopieur : (613) 990-5230
Site Web : http://www.sirc-csars.gc.ca
Les appels à frais virés sont acceptés et le standard téléphonique est ouvert de 8 h 00 à 17 h 30, heure normale de l'Est.

Nota : Aux fins du présent document, la forme masculine désigne, s'il y a lieu, aussi bien les femmes que les hommes.

© Travaux publics et Services gouvernementaux Canada 2001
N° de cat. JS71-1/2001
ISBN 0-662-65978-3

L'honorable Lawrence MacAulay, C.P., député
Solliciteur général du Canada
Chambre des communes
Ottawa (Ontario)
K1A 0A6

Le 30 septembre 2001

Monsieur le Ministre,

Conformément à l'article 53 de la *Loi sur le Service canadien du renseignement de sécurité*, nous présentons au Parlement, par votre entremise, le rapport du Comité de surveillance des activités de renseignement de sécurité pour l'exercice 2000–2001.

Veuillez agréer, Monsieur le Ministre, l'expression de notre haute considération.

La présidente,
Paule Gauthier, C.P., O.C., c.r.

James Andrews Grant, C.P., c.r.

Robert Keith Rae, C.P., O.C., c.r.

Raymond Speaker, C.P., O.C.

Frank McKenna, C.P.

Table des matières

Déclaration du Comité vii

Agencement du rapport annuel de vérification du CSARS x

Section 1 : Examen des activités de renseignement du SCRS 3

A. Dossiers d'intérêt particulier pour 2000–2001 3
Liaison du SCRS avec les organismes étrangers 3
Les instructions du Ministre – révision et mise à jour 8
Échanges d'informations au Canada (5) 9
Examen de la préparation des mandats 11
Notes d'évaluation de sécurité à CIC 12

B. Examen annuel des activités du SCRS dans une région 16
Autorisation des enquêtes 16
Exécution des mandats 18
Examen d'opérations délicates 19
Sécurité interne 20

C. Au sein du SCRS 21
Les mandats : généralités et données statistiques 21
Les organes opérationnels du SCRS 23
Ententes avec les ministères et les gouvernements 25
La collecte de renseignements étrangers 27

Section 2 : Filtrage de sécurité et enquêtes sur les plaintes 31

A. Filtrage de sécurité 33

B. Enquêtes sur les plaintes 37

Section 3 : Régime de responsabilisation du SCRS 41

A. Les rouages de la responsabilisation du SCRS 43

B. Au sein du CSARS 46

Annexe A : Sigles employés dans le rapport 49

Annexe B : Rapports et études du CSARS depuis 1984 53

Annexe C : Recommandations et principales constatations 65

Annexe D : Résumé des plaintes 71

Déclaration du Comité 2000-2001

Les événements survenus le 11 septembre 2001 aux États-Unis auront dissipé tout doute qui pouvait subsister quant au fait que les menaces les plus graves à la sûreté du Canada et à la sécurité de ses citoyens prennent des formes fort différentes de celles qu'a connues la génération précédente. Il y a environ seize ans, à l'époque du dernier remaniement de l'appareil national du renseignement de sécurité, la politique militaire singulière de la guerre froide était la toute première préoccupation. Aujourd'hui, nous vivons tous dans un monde marqué au coin de diverses forces nouvelles qui changent rapidement.

Personnes, capitaux, information, technologies et idéologies politiques sont plus mobiles que jamais. Pour la plupart, les influences qui en découlent sont réjouissantes ou du moins salutaires, mais d'autres ne le sont résolument pas. Par sa qualité de pays démocratique qui favorise les rapports et les investissements internationaux et qui accueille visiteurs et immigrants, le Canada s'expose à la fois aux meilleures et aux pires de ces influences.

Ce changement profond dans la nature des menaces se reflète dans tous les domaines de la politique publique qui touchent les intérêts nationaux du Canada et la sécurité de ses citoyens :

- Dans les instructions ministérielles données à la collectivité nationale du renseignement de sécurité, la violence à des fins politiques et le terrorisme figurent nettement à titre de menaces les plus sérieuses pour le Canada, les Canadiennes et les Canadiens.

- Au Service canadien du renseignement de sécurité, le déploiement des ressources, tant humaines que financières, traduit la nécessité croissante de faire face à de multiples menaces terroristes.

- Dans ses rapports publics des dernières années, le Service se dit de plus en plus préoccupé par le terrorisme et par un cadre de sécurité internationale qui favorise la conduite d'activités terroristes au Canada et à l'étranger.

- Les changements législatifs proposés et apportés par le gouvernement fédéral (projets de loi C-16, modifiant la *Loi de l'impôt sur le revenu*, et C-11, la *Loi sur l'immigration*) témoignent dans les deux cas de craintes que la violence à caractère politique ne soit dirigée ou financée de l'intérieur du Canada.

- *Le Rapport du Comité spécial du Sénat sur la sécurité et les services de renseignement* (Kelly, 1999), dernière étude du Parlement sur les questions de renseignement de sécurité, traite presque exclusivement de terrorisme et de violence à caractère politique et reste laconique quant aux menaces de l'espionnage.

Bref, en une dizaine d'années à peine, le SCRS, jadis voué surtout à lutter contre l'espionnage en faisant échec aux activités de collecte de renseignements d'un nombre assez limité de gouvernements étrangers, se préoccupe désormais avant tout du terrorisme et des politiques qui sous-tendent ce phénomène.

Les « cas » dont doit traiter le Service l'obligent à porter des jugements nuancés au sujet d'organismes et de personnes qui ont des visées politiques

Les modalités complexes de cette mutation sont patentes. Les « cas » dont doit traiter le Service l'obligent de plus en plus à porter des jugements nuancés – en raison de la ligne de démarcation souvent floue qui sépare les actions à caractère licite, politique ou illicite, teintées de violence ou de menaces de violence – au sujet des organismes et des personnes qui ont des visées politiques. Comme il appartient au Comité d'examiner et d'évaluer la qualité des jugements du SCRS en cette matière et que les priorités de celui-ci ont changé, les nôtres aussi ont évolué.

Pour le Comité, les questions d'action politique licite ou illicite et d'« association » à une organisation terroriste prennent une importance plus grande que jamais dans ses fonctions de surveillance et de tribunal chargé d'examiner les plaintes. Sur ces deux plans, son travail s'est transformé radicalement depuis 15 ans, ou même 10, et n'a pas fini d'évoluer. Les menaces terroristes, qui émanent de sources nouvelles et

divergentes, confèrent une grande importance à la compréhension des événements lorsqu'ils se produisent un peu partout dans le monde. Au moment où le SCRS réoriente ses efforts, le CSARS continuera de moduler en conséquence l'accent qu'il donne à ses recherches et les ressources qu'il y consacre.

Les fonctions du Comité à titre de tribunal chargé d'instruire les plaintes ont aussi évolué sensiblement. Une proportion croissante de plaintes concerne des questions de filtrage lié à l'immigration et à la sécurité qui portent pour la plupart sur des évaluations du Service à l'égard de personnes nourrissant des visées politiques et qui nécessitent de longues investigations sur les activités, les sources de renseignement et les cultures politiques d'autres pays. Si les projets de loi C-16 et C-11 entrent en vigueur, le CSARS craint de voir ces plaintes se multiplier.

Le Comité ne croit en l'existence d'aucune solution politique ou législative magique qui rende ces jugements moins difficiles à porter ou facilite l'atteinte d'un juste milieu entre la sécurité nationale et la protection des droits civils. En vertu de la politique nationale actuelle, le Service est tenu d'enquêter sur les menaces dont le gouvernement doit être informé, selon son évaluation professionnelle de la gravité de chacune. Quant aux évaluations du CSARS, elles sont aussi fondées sur l'expérience et le savoir professionnels, et non sur des guides d'orientation. Le Comité ne croit pas, non plus, qu'il soit bien utile de définir avec précision les termes « terroriste », « association » ou « extrémisme », surtout dans un contexte mondial où les changements semblent se faire chaque jour plus rapides.

Le Comité ne croit en l'existence d'aucune solution politique ou législative magique qui rende ces jugements moins difficiles à porter

Le CSARS confère toutefois un éclairage particulier aux dilemmes entourant le renseignement de sécurité – ce qui était précisément l'intention du Parlement. Le SCRS représente le droit et la responsabilité du gouvernement de protéger la vie des citoyens et de maintenir l'ordre public. Le CSARS incarne, entre autres, un principe juridique essentiel de la démocratie canadienne, soit que les citoyens ont le droit à la vie privée et des libertés civiles et sont soustraits au pouvoir gouvernemental sans entrave – la « liberté de l'individu ».

La complexité et l'ambiguïté qui ont fini par dominer le travail dans le domaine du renseignement de sécurité signifient qu'une proportion plus grande que jamais des pouvoirs de jugement du Service – et, par conséquent, du Comité – sert à

prendre des décisions qui sont vitales pour préserver tant la liberté des Canadiennes et des Canadiens que leur sécurité. Le terrorisme est un outrage à la démocratie; pour y faire échec, il faudra à la fois consolider sensiblement la coopération et la détermination internationales et promouvoir sans relâche les valeurs fondamentales du Canada.

Agencement du rapport annuel de vérification du CSARS

Le rapport est agencé selon les principales fonctions du Comité : examiner les activités de renseignement du SCRS, faire enquête sur les plaintes relatives au Service et sur les questions connexes et, de concert avec d'autres rouages de l'appareil gouvernemental, protéger les Canadiens contre les menaces pour leur sécurité.

- La section 1 contient les résultats de l'examen et de la vérification, par le CSARS, de ce que fait le Service et de la manière dont il le fait. Aux diverses subdivisions correspondent les méthodes généralement employées par le Comité pour faire ces évaluations.

- La section 2 traite du rôle du CSARS en qualité de tribunal quasi judiciaire, investi du pouvoir d'enquêter sur diverses catégories de plaintes.

- La section 3 englobe sous une même rubrique – Régime de responsabilisation du SCRS – les multiples mécanismes administratifs et juridiques, étudiés par le Comité, par lesquels le Service rend compte au gouvernement, au Parlement et à la population du Canada.

Comme les rapports précédents, celui de cette année établit une distinction nette entre les commentaires et recommandations qui découlent de la tâche principale du Comité – scruter le SCRS et ses activités échelonnées sur une certaine période – et les renseignements plus généraux ou historiques qu'il fournit aux Canadiens et aux autres lecteurs pour les aider à saisir le contexte dans lequel baigne le travail du renseignement de sécurité.

Les sujets qui, de l'avis du CSARS, intéressent le lecteur par leur caractère informatif, documentaire ou technique figurent dans des encadrés ombrés. Contrairement au corps du rapport, ces textes ne contiennent aucune opinion ni conclusion du Comité et visent à exposer des faits.

Dans chaque section du rapport de vérification, une innovation mineure, quoique importante à nos yeux, est la mention de l'étude du CSARS dont chacune est tirée, le cas échéant. Les références complètes des études figurent à l'annexe B.

prendre des décisions qui sont vitales pour préserver tant la liberté des Canadiennes et des Canadiens que leur sécurité. Le terrorisme est un outrage à la démocratie; pour y faire échec, il faudra à la fois consolider sensiblement la coopération et la détermination internationales et promouvoir sans relâche les valeurs fondamentales du Canada.

Agencement du rapport annuel de vérification du CSARS

Le rapport est agencé selon les principales fonctions du Comité : examiner les activités de renseignement du SCRS, faire enquête sur les plaintes relatives au Service et sur les questions connexes et, de concert avec d'autres rouages de l'appareil gouvernemental, protéger les Canadiens contre les menaces pour leur sécurité.

- La section 1 contient les résultats de l'examen et de la vérification, par le CSARS, de ce que fait le Service et de la manière dont il le fait. Aux diverses subdivisions correspondent les méthodes généralement employées par le Comité pour faire ces évaluations.

- La section 2 traite du rôle du CSARS en qualité de tribunal quasi judiciaire, investi du pouvoir d'enquêter sur diverses catégories de plaintes.

- La section 3 englobe sous une même rubrique – Régime de responsabilisation du SCRS – les multiples mécanismes administratifs et juridiques, étudiés par le Comité, par lesquels le Service rend compte au gouvernement, au Parlement et à la population du Canada.

Comme les rapports précédents, celui de cette année établit une distinction nette entre les commentaires et recommandations qui découlent de la tâche principale du Comité – scruter le SCRS et ses activités échelonnées sur une certaine période – et les renseignements plus généraux ou historiques qu'il fournit aux Canadiens et aux autres lecteurs pour les aider à saisir le contexte dans lequel baigne le travail du renseignement de sécurité.

Les sujets qui, de l'avis du CSARS, intéressent le lecteur par leur caractère informatif, documentaire ou technique figurent dans des encadrés ombrés. Contrairement au corps du rapport, ces textes ne contiennent aucune opinion ni conclusion du Comité et visent à exposer des faits.

Dans chaque section du rapport de vérification, une innovation mineure, quoique importante à nos yeux, est la mention de l'étude du CSARS dont chacune est tirée, le cas échéant. Les références complètes des études figurent à l'annexe B.

Section 1

Examen des activités de renseignement du SCRS

Examen des activités de renseignement du SCRS

A. Dossiers d'intérêt particulier pour 2000–2001

Liaison du SCRS avec les organismes étrangers

Rapport n° 2000-03

CONTEXTE

Comme il est prévu au sous-alinéa 38a)(iii) de la *Loi sur le Service canadien du renseignement de sécurité*, le Comité de surveillance des activités de renseignement de sécurité (CSARS) examine les ententes de coopération et d'échange d'informations que le SCRS conclut avec des services de renseignement et de police étrangers ainsi que les informations qu'il leur communique.

Cette année, l'examen du CSARS visait un bureau d'agent de liaison-sécurité (ALS) qui œuvre à l'étranger dans un milieu particulièrement difficile. C'est un défi de taille d'assurer la sécurité du cadre physique de fonctionnement de ce bureau où les conditions de travail généralement pénibles empirent la situation.

Le SCRS a ouvert ce bureau avec la conviction qu'un engagement constructif, fondé sur le dialogue et sur l'échange d'informations, l'aiderait à s'acquitter de son mandat en matière de sécurité nationale. Il s'est employé à chercher des terrains communs particuliers où les informations ainsi échangées pourraient favoriser les intérêts canadiens et il a qualifié de « prudente » et « mesurée » – c'est-à-dire favorisant la transparence et la coopération – son approche à l'égard de cette relation.

MÉTHODE D'EXAMEN

La vérification effectuée par le Comité a porté sur trois catégories de documents :

- tous les échanges d'informations effectués à ce bureau par l'ALS du SCRS, dont ceux par voie électronique;
- toute la correspondance avec des organismes de renseignement étrangers traitée à ce bureau; et
- l'ensemble des instructions et documents de référence reçus ou envoyés par l'ALS, y compris ses « évaluations d'organismes étrangers ».

Les objectifs essentiels de l'examen étaient de vérifier si les relations et contacts avec les organismes étrangers concernés étaient conformes aux ententes particulières en matière de liaison et si le Service avait traité comme il fallait les informations fournies ou reçues.

De façon plus générale, le Comité a scruté les activités au bureau choisi dans le contexte de l'ensemble du programme de liaison du Service avec l'étranger, y compris les instructions du Ministre et les politiques du SCRS. Comme il l'avait fait lors d'examens antérieurs des activités de liaison du Service avec l'étranger, le CSARS a porté une attention spéciale aux échanges d'informations qui auraient pu amener des tiers à violer les droits de la personne.

POLITIQUES ET ADMINISTRATION

Dans l'ensemble, les politiques de liaison avec l'étranger sont énoncées dans des instructions du Ministre; pour la période à l'étude, l'instruction pertinente avait été donnée en 1982. Comme il est prescrit à l'article 17 de la *Loi sur le SCRS*, le Service peut conclure des ententes de coopération avec des organismes d'autres pays. Le Comité examine ces ententes dans lesquelles sont définies la nature et la portée de chacune.

La conclusion d'ententes de liaison avec des services de renseignement étrangers doit être approuvée par le solliciteur général après consultation du ministre des Affaires étrangères et du Commerce international. L'entente à laquelle sont assujettis les échanges au bureau choisi pour la vérification de cette année a été signée au cours de la dernière décennie.

Nouvelle instruction du Ministre

Comme on l'a vu plus haut, l'instruction ministérielle concernant la période à l'étude remonte à 1982. Depuis la vérification du Comité au bureau d'A[illegible] visé, le Ministre a toutefois donné une nouvelle instruction couvrant toutes les opérations du SCRS, y compris les ententes de liaison avec l'étranger. Dans son rapport de 1997–1998, le Comité a jugé nécessaire que le gouvernement mette à jour cette instruction, notamment en ce qui touche les activités de liaison avec l'étranger, et il a recommandé que le Service revoie toutes ses ententes pour en assurer la conformité au nouveau cadre, dès que celui-ci serait instauré. Dans son examen de la nouvelle instruction ministérielle, le Comité s'est attaché tout particulièrement aux éléments touchant la liaison avec l'étranger, compte tenu de ses propos antérieurs. (Voir à la page 8 l'exposé complet sur cette instruction.)

Pour ce qui est de la liaison avec l'étranger, la nouvelle instruction du Ministre semble reprendre les orientations clés de l'ancienne, c'est-à-dire que :

- les ententes nécessaires pour assurer la sécurité du Canada peuvent être conclues;
- ces ententes doivent être approuvées par le solliciteur général en consultation avec le ministre des Affaires étrangères et du Commerce international;
- il faut évaluer la réputation du pays ou organisme en cause quant au respect des droits de la personne et tenir compte de cette évaluation dans toute décision de conclure une entente de coopération;
- les ententes doivent être conformes aux lois applicables du Canada et en accord avec sa politique étrangère.

Dans la nouvelle instruction ministérielle, le seul point sensiblement différent de la précédente est le pouvoir discrétionnaire élargi qui est accordé au directeur du SCRS pour gérer les ententes de coopération. On y lit en effet que le « directeur doit assurer la gestion de ces ententes conformément aux conditions imposées par le ministre », tandis que l'ancienne conférait à celui-ci la charge d'arrêter les paramètres précis de la coopération.

La nouvelle instruction accorde un pouvoir discrétionnaire élargi au directeur du SCRS dans la gestion des ententes de coopération

Comme le Ministre n'a donné sa nouvelle instruction qu'en février 2001, il faudra quelque temps au Comité pour évaluer les implications des politiques révisées, surtout quant au pouvoir discrétionnaire élargi du directeur. Dans l'ensemble, nous croyons toutefois que cette instruction est une nette amélioration sur les précédentes, car la terminologie y est plus simple et conforme à celle de la législation qui régit l'ensemble des activités du SCRS.

À l'occasion de l'examen des ententes de liaison avec l'étranger, en 1997–1998 – et en prévision de la nouvelle instruction du Ministre – le Comité avait recommandé que le Service les réexamine toutes systématiquement afin d'en assurer la conformité à la nouvelle instruction, dès qu'elle serait donnée. Le Service a informé le CSARS qu'il ferait la prochaine évaluation annuelle de toutes ses ententes de liaison à la lumière de cette instruction.

CONSTATATIONS AU BUREAU CHOISI

Vue d'ensemble

Au cours de la vérification du Comité au bureau de l'ALS, nous avons été frappés par les piètres conditions dans lesquelles le personnel du Service doit travailler. Des installations déficientes, combinées à la lourde charge de travail occasionnée par la multiplication des demandes d'immigration et de visa requérant un filtrage de sécurité, suscitent un climat défavorable. En dépit de ces circonstances difficiles, l'ALS et le personnel du bureau canadien font du bon travail.

Nous avons constaté que l'ALS a fait des progrès constants auprès des interlocuteurs étrangers; cependant, comme le volet immigration de son mandat l'accapare de plus en plus, il lui reste moins de temps pour nouer des relations avec les autres pays dont il est théoriquement chargé dans la région.

Activités de filtrage

L'examen des ressources attribuées à ce bureau montre au Comité que le personnel doit consacrer de plus en plus de temps au filtrage de sécurité des demandes d'immigration et de visa. En l'espace de quelques mois, la charge de travail s'est beaucoup alourdie sur ce plan, à tel point que le Service a dû y affecter temporairement des employés supplémentaires. Les piètres installations et le milieu difficile sur le plan de la sécurité ont compliqué davantage les choses.

> Nous avons été frappés par les piètres conditions dans lesquelles le personnel du Service doit travailler

La charge de travail manifestement trop lourde a fait craindre au Comité que certaines fonctions importantes du bureau puissent ne pas être remplies promptement. La haute direction du Service a dit au CSARS qu'elle partageait ces craintes et qu'à son avis ce problème, côté immigration, était commun à certains autres bureaux d'ALS.

Au début des années 90, le Service et un autre organisme fédéral ont effectué une étude conjointe des tâches liées à l'immigration, dans des bureaux situés à l'étranger, ce qui a permis de mieux cibler l'utilisation des services des agents du SCRS. Le Comité est d'avis que le Service voudra peut-être scruter à nouveau cet élément de son Programme de liaison avec l'étranger. Pour sa part, lors de ses prochaines vérifications, il compte examiner les fonctions liées au filtrage de sécurité dans des bureaux d'ALS choisis à l'étranger.

Échanges d'informations

Le Comité a examiné toute la documentation ayant trait à la coopération opérationnelle et aux échanges d'informations auxquels avait pris part le bureau d'ALS entre le 31 mars 1998 et le 30 juin 2000. Les échanges d'informations du Service avec les organismes étrangers que dessert ce bureau ont été examinés pour vérifier si les informations que celui-ci leur avait fournies ou en avait reçues avaient été traitées comme il faut.

Notre examen a révélé un seul échange problématique. Des clients du Service en avaient reçu des renseignements tendancieux – de fiabilité douteuse, selon le Comité – sur une personne. Après avoir signalé la chose au SCRS, celui-ci nous a fourni des éclaircissements. Nous lui avons dit qu'il devrait songer à transmettre ces éclaircissements à ses clients pour qu'ils puissent replacer l'opinion antérieure dans le bon contexte.

Organismes étrangers et droits de la personne

La crainte de répercussions sur le plan des droits de la personne était à l'avant-plan de la vérification de ce bureau par le Comité. Par contre, il y avait l'impératif fondamental et primordial de conclure des ententes avec des services de renseignement étrangers : le SCRS doit en effet recueillir les informations requises pour protéger les Canadiens.

À plusieurs reprises ces dernières années, le Comité a élaboré sa position au sujet des rapports du SCRS avec les organismes étrangers. À son avis, le Service doit veiller par tous les moyens à éviter que les informations qu'il communique puissent servir à favoriser la violation des droits de la personne. À cette fin, les ALS sont tenus de fournir au reste du SCRS des évaluations exactes et à propos sur la réputation des organismes, et cela, sur deux plans : le respect des droits de la personne et la tendance à transmettre sans autorisation ces informations à des tiers. Le Service doit éviter les situations où il fournit de l'information à un organisme qui ne viole pas les droits de la personne pour constater ensuite que l'information est transmise à d'autres organismes moins scrupuleux à ce sujet.

Pour ce qui est du bureau d'ALS soumis à la vérification, le Comité n'a trouvé aucun échange d'informations qui ne respectait pas ces normes et il est convaincu que toutes les évaluations d'organismes en matière de respect des droits de la personne ont été effectuées selon les règles de l'art.

Instructions du Ministre – révision et mise à jour

En février 2001, le solliciteur général a diffusé un recueil d'instructions ministérielles révisées sur la gestion du Service – ce que le Comité souhaitait depuis un certain temps déjà.

L'ÉVOLUTION DES INSTRUCTIONS DU MINISTRE

Selon l'article 6 de la *Loi sur le SCRS*, le directeur du Service est « chargé de la gestion » de cet organisme suivant les directives du Ministre – soit le solliciteur général du Canada. La prestation de ces directives se fait principalement par écrit au moyen d'« instructions du Ministre ». La Loi prévoit qu'un exemplaire de ces instructions doit être transmis au Comité « dès qu'elles sont données ».

Les instructions du Ministre visent un vaste éventail d'activités du Service : des orientations stratégiques aux conseils sur des questions particulières telle la conduite d'enquêtes concernant des institutions névralgiques. À l'occasion de vérifications antérieures, le Comité a examiné la valeur d'instructions particulières, la manière dont le Service les avait transposées dans ses propres politiques et procédures et leur mise en œuvre dans des cas donnés.

> Les directives ministérielles sont considérablement simplifiées et uniformes quant au language employé

Une chose qui a souvent préoccupé le Comité est le caractère disparate et morcelé de ces instructions prises globalement. Au fil des dix-sept années d'existence du Service, des ministres ont souvent donné des instructions sur des questions particulières au moment où celles-ci se produisaient. Certaines instructions, toujours valables à titre d'orientations ministérielles, précèdent en fait la création du SCRS. Il en avait résulté un fatras d'orientations stratégiques où l'on trouvait un langage parfois contradictoire et une terminologie qui ne concordait plus avec la législation.

LES NOUVELLES INSTRUCTIONS : VUE D'ENSEMBLE

Le nouveau recueil (document classifié), qui remplace intégralement les anciennes instructions, rationalise passablement l'orientation stratégique du Service par le gouvernement et, de l'avis du Comité, témoigne d'une maturation du cadre légal et stratégique qui régit le travail du SCRS. Les directives ministérielles sont désormais considérablement simplifiées et uniformes quant au langage employé et forment un document concis et cohérent.

Naturellement, il est trop tôt pour évaluer l'impact des instructions révisées sur les opérations du Service. La brièveté relative du recueil et le caractère stratégique des instructions donnent à penser qu'on mettra davantage l'accent sur les politiques opérationnelles mêmes du SCRS comme source d'instructions et de lignes directrices particulières à suivre. Il est en outre manifeste qu'il y a eu un transfert global de pouvoirs discrétionnaires du cabinet du solliciteur général au directeur du Service, quant à la gestion courante du SCRS. Lors de vérifications futures, le Comité compte porter une attention particulière à la manière dont les nouvelles instructions seront interprétées et appliquées à l'ensemble des activités du Service.

Échanges d'informations au Canada (5)

Rapport nº 2001-01

Dans l'exercice de ses fonctions d'enquête sur les menaces présumées à l'égard de la sécurité du Canada, le Service coopère avec les ministères et organismes fédéraux et provinciaux ainsi qu'avec les services de police de l'ensemble du pays et il échange des informations avec eux. C'est l'article 17 de la *Loi sur le SCRS* qui lui octroie le mandat de conclure des ententes à cette fin, tandis que le paragraphe 19(2) de cette loi l'habilite à communiquer des informations à divers ministères et organismes canadiens « en vue de l'exercice des fonctions qui lui sont conférées ».

En vertu du sous-alinéa 38a)(iii) de la Loi, le Comité est chargé d'examiner les accords de coopération que le Service conclut avec des organismes canadiens ainsi que les informations et renseignements que celui-ci leur fournit aux termes de ces accords.

PORTÉE ET MÉTHODE DE L'EXAMEN

Le Comité a examiné tous les échanges d'informations du Service avec les autres organismes canadiens, y compris les informations accessoires qu'il leur a fournies pendant l'exercice 1999–2000. Il a en outre scruté sur place les pratiques suivies dans un bureau régional du SCRS en matière d'échanges.

L'examen visait à déterminer si, dans ses échanges d'informations avec les organismes canadiens, le Service s'était conformé aux instructions ministérielles, aux protocoles d'entente conclus avec les institutions gouvernementales et avec les services de police, à ses politiques opérationnelles, à la *Loi sur le SCRS* et aux autres lois pertinentes. Dans son investigation, le Comité a notamment examiné :

- si la menace requérant communication de renseignements primait suffisamment sur les attentes raisonnables du public en matière de protection de la vie privée,
- si les échanges d'informations étaient strictement nécessaires pour répondre aux besoins opérationnels du Service, selon l'article 12 de la *Loi sur le SCRS*,
- si ces échanges supposaient utilisation abusive de renseignements personnels et délicats,
- si les informations échangées étaient raisonnables et conformes aux faits,
- si toutes les communications d'informations du SCRS à d'autres organismes se situaient dans les limites énoncées au paragraphe 19(2) de la *Loi sur le SCRS*, et
- si tous les échanges d'informations étaient consignés de façon uniforme.

CONSTATATIONS DU COMITÉ

Coopération générale

Pour la période à l'étude, le Comité a relevé deux échanges d'informations préoccupants. Tous les autres respectaient le mandat du Service et les politiques existantes. Les informations échangées étaient raisonnables et conformes aux faits, ne supposaient aucune utilisation abusive de renseignements personnels et délicats et n'empiétaient pas indûment sur la vie privée.

Conservation d'informations non sollicitées

Les deux cas qui ont attiré l'attention du Comité ont tous deux été relevés à l'occasion de la vérification faite dans un bureau régional du SCRS et ont trait à la gestion d'informations reçues d'organismes canadiens.

Dans le premier cas, la base de données dans laquelle le Service avait versé les informations non sollicitées contenait plusieurs documents concernant des personnes et des organisations sur lesquelles il n'était pas autorisé à enquêter. Nous avons demandé au SCRS pourquoi il avait conservé ces documents et ses explications nous ont satisfaits. Le Comité croit toutefois que les raisons de conserver des informations non sollicitées d'une telle nature devraient, à l'avenir, être énoncées clairement dans les rapports opérationnels pertinents.

> **Le Comité recommande que les raisons pour lesquelles des informations sont conservées dans une catégorie générale soient énoncées clairement dans les rapports opérationnels.**

Depuis, le Service s'est rallié à notre recommandation et nous a informés que la partie pertinente des politiques sur les opérations sera modifiée en conséquence.

Le deuxième cas qui a attiré notre attention concernait l'opportunité de conserver certaines informations reçues d'un organisme canadien. Il s'agit de dossiers qui avaient trait aux activités d'un petit groupe de mineurs. Le Service a dit au Comité qu'il avait d'abord conservé ces dossiers parce qu'ils montraient que le groupe était enclin à se livrer à des actes de violence grave contre des personnes ou des biens dans le but d'atteindre un objectif politique – menace qui entre dans le mandat du SCRS. Après avoir réévalué les informations reçues initialement, le Service a alors décidé qu'aucune autre mesure ne s'imposait; il les a toutefois conservées.

Le Comité reconnaît pleinement que le Service a charge d'enquêter sur toute information, reçue d'autres organismes, qui semble entrer dans son mandat. Nous nous demandons toutefois s'il y avait lieu de conserver l'information, dans ce cas-là, une fois prise la décision de ne pas pousser l'enquête plus loin. Le CSARS est d'avis que les informations en cause devraient être retirées des dossiers du SCRS.

Quant au Service, il a réaffirmé qu'il y avait lieu initialement, à son avis, de conserver les informations et il a précisé que le maintien de cette décision préservait officiellement les informations reçues et les mesures prises. Le SCRS a convenu de modifier les rapports opérationnels de manière à refléter sa décision finale selon laquelle les informations ne justifiaient aucune autre mesure de sa part.

Le Comité recommande que le Service fasse preuve d'une plus grande diligence lorsqu'il décide s'il doit conserver des informations non sollicitées.

Examen de la préparation des mandats

Rapport n° 2000-05

Pour obtenir des pouvoirs par la voie d'un mandat en vertu de l'article 21 de la *Loi sur le SCRS*, le Service rédige à l'intention de la Cour fédérale une demande à laquelle il joint une déclaration sous serment, ou affidavit, exposant les raisons qui justifient le recours à des techniques intrusives pour enquêter sur une menace particulière à la sécurité du Canada. Comme la bonne préparation des affidavits est clé pour assurer l'intégrité du processus, le Comité examine périodiquement un certain nombre de mandats, choisis parmi ceux qui étaient en vigueur pendant la période à l'étude.

Même s'il appartient en propre à la Cour fédérale de décerner les mandats et de les assortir des conditions qu'elle juge appropriées, le Comité a un double objectif en surveillant la préparation des mandats par le Service :

- veiller à ce que les faits exposés dans les affidavits soient conformes à l'information qui a servi à les rédiger, et
- veiller à ce que les faits, circonstances et déclarations dont il est fait état dans les affidavits soient présentés de façon juste et objective.

Parmi les mandats décernés en 1999–2000, le Comité en a retenu deux en vue d'un examen détaillé – l'un concernait une cible de l'antiterrorisme et l'autre, une enquête de contre-espionnage. Le Comité a étudié tous les documents du SCRS ayant trait à la préparation des affidavits : dossiers généraux de mandats, classeurs de « documents sources », messages internes, demandes d'autorisation d'enquête, procès-verbaux de réunions du Comité d'approbation et de réévaluation des cibles (CARC) et affidavits mêmes.

Dans chacun des cas choisis, le CSARS a trouvé que l'affidavit présenté par le Service à la Cour fédérale était en accord avec les faits exposés dans les pièces justificatives et que les faits et circonstances énoncés dans l'affidavit étaient présentés de façon juste et objective.

RÉVISION DES DISPOSITIONS ET CONDITIONS DES MANDATS

Comme nous le mentionnions dans le rapport de l'an dernier [référence], le Service a entrepris une révision globale des dispositions et des conditions des mandats pour en simplifier la terminologie et les harmoniser avec la législation actuelle. Certaines procédures opérationnelles et administratives ont aussi été modifiées.

Le SCRS a signalé au Comité que ce processus avait été mené à terme et qu'il avait pleinement informé tout son personnel chargé de demander ou d'exécuter les mandats. La Cour fédérale a approuvé tous les changements dont tenaient compte les demandes de mandat ultérieures.

Notes d'évaluation de sécurité à CIC

Rapport n° 2001-02

L'objet de cette étude était d'évaluer l'information que le SCRS fournit au ministre de la Citoyenneté et de l'Immigration du Canada (CIC) dans le cadre du rôle qui lui échoit en vertu de son mandat, soit prêter main-forte à l'égard du programme

gouvernemental de surveillance de l'immigration au moyen de services de filtrage de sécurité. C'est dans son rapport de 1997–1998 que le Comité a examiné pour la dernière fois le rôle du Service en matière d'immigration. Cette année, il s'est attaché spécialement à la nature et à la qualité des conseils que le SCRS fournit à CIC sous forme de notes d'information.

MÉTHODE D'EXAMEN

Pour cette étude, le Comité a examiné seize enquêtes de sécurité à l'immigration menées par le Service et choisies à partir des 166 notes d'information que le SCRS avait envoyées à CIC au cours de l'exercice 1999–2000. Cet échantillon comprend neuf dossiers d'origine canadienne et sept provenant de l'étranger. Le CSARS a étudié les notes d'information envoyées à CIC et toutes les pièces justificatives concernant chaque enquête.

MODALITÉS DE LA PRESTATION DE CONSEILS PAR LE SERVICE

Le SCRS a la responsabilité exclusive de fournir des évaluations de sécurité à l'égard des demandes d'immigration présentées au Canada et aux États-Unis. Pour celles provenant d'ailleurs, il appartient au gestionnaire du Programme d'immigration de la mission canadienne compétente à l'étranger de demander une telle évaluation au Service. Dans les deux cas, indépendamment des conseils donnés par le SCRS à CIC, c'est au ministre de la Citoyenneté et de l'Immigration qu'il appartient de prendre la décision finale quant à l'admissibilité de tout immigrant éventuel.

Généralement, une enquête de filtrage de sécurité à l'immigration est ouverte lorsque le Service reçoit une demande d'un centre de traitement de données au Canada ou du gestionnaire du Programme d'immigration d'une mission canadienne à l'étranger et elle prend fin lorsque le SCRS donne son opinion à CIC sous l'une des quatre formes suivantes :

Rien à signaler – rapport remis à CIC si le Service n'a aucun renseignement défavorable sur l'immigrant éventuel.

Avis de non-admissibilité – opinion dans les cas où le Service conclut, d'après les renseignements dont il dispose, que le demandeur répond aux critères énoncés dans les dispositions de l'article 19 de la *Loi sur l'immigration* concernant la sécurité.

Note d'information – opinion du SCRS affirmant avoir en main des informations selon lesquelles le demandeur trempe ou a trempé dans des activités visées par les dispositions de la *Loi sur l'immigration* qui ont trait à la sécurité, mais exprimant l'avis que l'intéressé n'entre pas dans la catégorie des personnes jugées non admissibles en vertu de cette loi.

Lettre d'anecdote – remise à CIC par le Service et signalant toute information qu'il a en main selon laquelle le demandeur prend ou a pris part à des activités non liées à la sécurité et décrites à l'article 19 de la *Loi sur l'immigration* – crimes de guerre ou criminalité organisée, par exemple – ou toute autre question ayant trait à l'exercice des fonctions du ministre de la Citoyenneté et de l'Immigration, conformément à l'alinéa 14b) de la *Loi sur le SCRS*.

CONSTATATIONS DU COMITÉ

Nature des opinions du Service

Toutes les notes d'information dans lesquelles le Service avait donné une opinion à CIC ont été jugées exactes et bien fondées sur les renseignements recueillis. Nous avons relevé un cas où le SCRS n'avait pu fournir d'opinion valable faute d'information suffisante.

> Toutes les notes d'information fournies à CIC ont été jugées exactes et bien fondées sur les renseignements recueillis

Dans l'ensemble, le Comité a constaté que le Service avait rédigé plus de notes d'information pour les dossiers d'origine canadienne que pour ceux provenant de l'étranger, en dépit du fait que la majorité des dossiers entrent dans cette dernière catégorie. Cette question sera examinée lors d'une prochaine vérification.

Statistiques essentielles

Au cours de l'exercice à l'étude, le Service a effectué 81 650 évaluations de filtrage de sécurité à l'immigration et, dans la majorité des cas, il n'a rien trouvé à signaler. Il a envoyé à CIC 166 notes d'information dont 109 étaient des avis de non-admissibilité. Il a fallu en moyenne au SCRS 661 jours pour traiter les dossiers de filtrage de sécurité à l'immigration qui ont donné lieu à une note d'information. Pour ceux qui ont abouti à un avis de non-admissibilité, le temps de traitement moyen a été de 644 jours. Les explications du Service au sujet des délais de traitement figurent à la section 2, sous la rubrique Filtrage de sécurité, à la page 33.

Faits récents

Dans son rapport pour 1997–1998, le Comité avait fait état de lacunes dans le processus de filtrage de sécurité des demandeurs du statut de réfugié au Canada. À son avis, le Service pouvait et devait jouer un rôle élargi afin de seconder les efforts de CIC en ce domaine.

Le Comité a appris récemment que le Service et CIC avaient instauré le programme « Filtrage dès le début du processus » pour les demandeurs du statut de réfugié au Canada. Au moment de présenter leurs demandes, tous les intéressés seront soumis à un processus de filtrage semblable à celui que doivent subir ceux qui demandent la résidence permanente. L'objet du programme est d'éviter que l'on puisse entrer au Canada et y demeurer pendant une période indéfinie sans subir d'évaluation de filtrage de sécurité – ce qui posait un risque important selon la procédure en place lors de notre examen précédent.

Le Comité suivra de près ce changement et les autres survenus récemment dans les rapports de coopération entre le SCRS et CIC.

« Motifs de soupçonner » « motifs de croire » Menaces à la sécurité et non-admissibilité, en droit canadien

Le Service aide CIC au titre du filtrage de sécurité en échangeant avec lui des informations sur les questions qui ont trait aux menaces envers la sécurité du Canada, au sens de l'article 2 de la *Loi sur le SCRS*, et en lui fournissant des avis quant aux catégories non admissibles en vertu de l'article 19 de la *Loi sur l'immigration*. Ce sont là des lois distinctes du Parlement qui contiennent des dispositions différentes – « menaces envers la sécurité du Canada » et « non-admissibilité au Canada » – et qui influent toutes deux sur les questions de sécurité liées à l'immigration.

Quiconque demande à immigrer au Canada peut être déclaré non admissible selon les critères énoncés à l'article 19 de la *Loi sur l'immigration*. Cependant, l'intéressé (immigrant éventuel ou autre) peut également correspondre aux critères qui font de lui une menace envers la sécurité du Canada, au sens de la *Loi sur le SCRS*.

Le critère de non-admissibilité en vertu de la *Loi sur l'immigration* est plus sévère que celui qui amène à ouvrir une enquête en vertu de l'article 12 de la *Loi sur le SCRS*. Pour mener une telle enquête, le Service doit avoir des motifs raisonnables de « soupçonner » une personne ou un groupe de menacer la sécurité du Canada. Par contre, pour que CIC refuse l'admission pour des raisons de sécurité, l'avis de non-admissibilité du SCRS doit corroborer sa conclusion à l'existence de motifs raisonnables de « croire » que le demandeur appartient à une catégorie non admissible – critère à respecter qui est plus strict en droit.

Dans ses notes d'information à CIC, le Service fournit une évaluation de l'admissibilité du demandeur par rapport à la *Loi sur l'immigration*. Il n'a toutefois pas pour rôle de déterminer si l'intéressé est une menace envers la sécurité du Canada, au sens de la *Loi sur le SCRS*.

Le Comité a appris récemment que le Service et CIC avaient instauré le programme « Filtrage dès le début du processus » pour les demandeurs du statut de réfugié au Canada. Au moment de présenter leurs demandes, tous les intéressés seront soumis à un processus de filtrage semblable à celui que doivent subir ceux qui demandent la résidence permanente. L'objet du programme est d'éviter que l'on puisse entrer au Canada et y demeurer pendant une période indéfinie sans subir d'évaluation de filtrage de sécurité – ce qui posait un risque important selon la procédure en place lors de notre examen précédent.

Le Comité suivra de près ce changement et les autres survenus récemment dans les rapports de coopération entre le SCRS et CIC.

« Motifs de soupçonner » « motifs de croire » Menaces à la sécurité et non-admissibilité, en droit canadien

Le Service aide CIC au titre du filtrage de sécurité en échangeant avec lui des informations sur les questions qui ont trait aux menaces envers la sécurité du Canada, au sens de l'article 2 de la *Loi sur le SCRS*, et en lui fournissant des avis quant aux catégories non admissibles en vertu de l'article 19 de la *Loi sur l'immigration*. Ce sont là des lois distinctes du Parlement qui contiennent des dispositions différentes – « menaces envers la sécurité du Canada » et « non-admissibilité au Canada » – et qui influent toutes deux sur les questions de sécurité liées à l'immigration.

Quiconque demande à immigrer au Canada peut être déclaré non admissible selon les critères énoncés à l'article 19 de la *Loi sur l'immigration*. Cependant, l'intéressé (immigrant éventuel ou autre) peut également correspondre aux critères qui font de lui une menace envers la sécurité du Canada, au sens de la *Loi sur le SCRS*.

Le critère de non-admissibilité en vertu de la *Loi sur l'immigration* est plus sévère que celui qui amène à ouvrir une enquête en vertu de l'article 12 de la *Loi sur le SCRS*. Pour mener une telle enquête, le Service doit avoir des motifs raisonnables de « soupçonner » une personne ou un groupe de menacer la sécurité du Canada. Par contre, pour que CIC refuse l'admission pour des raisons de sécurité, l'avis de non-admissibilité du SCRS doit corroborer sa conclusion à l'existence de motifs raisonnables de « croire » que le demandeur appartient à une catégorie non admissible – critère à respecter qui est plus strict en droit.

Dans ses notes d'information à CIC, le Service fournit une évaluation de l'admissibilité du demandeur par rapport à la *Loi sur l'immigration*. Il n'a toutefois pas pour rôle de déterminer si l'intéressé est une menace envers la sécurité du Canada, au sens de la *Loi sur le SCRS*.

B. Examen annuel des activités du SCRS dans une région

Chaque année, le Comité examine l'éventail complet des activités d'enquête du SCRS – ciblage, opérations spéciales, mandats, entrevues de dirigeants de groupes ethniques et d'intérêt et opérations délicates – dans une région donnée du Canada. Pareil tour d'horizon l'éclaire sur l'usage que le Service fait des divers outils dont il dispose pour ses enquêtes et lui permet d'évaluer comment les organes opérationnels du SCRS appliquent les instructions ministérielles et les politiques du Service.

Autorisation des enquêtes

Dans la surveillance des régions, la partie autorisation des enquêtes porte sur l'exercice des fonctions conférées au Service en vertu des articles 2 et 12 de la Loi. La gestion courante des enquêtes est régie à la fois par les instructions du Ministre et par les politiques opérationnelles du SCRS.

Pour déterminer si les enquêtes du Service sont légitimes, le Comité se fonde sur trois critères principaux :

1) Le SCRS avait-il des motifs raisonnables de soupçonner l'existence de menaces à l'égard de la sécurité du Canada?

2) Le niveau et le degré d'intrusion des enquêtes étaient-il proportionnels à la gravité des menaces représentées par les activités?

3) Le Service a-t-il recueilli uniquement les informations dont il avait strictement besoin pour remplir son mandat visant à informer le gouvernement de l'existence de menaces?

MÉTHODE D'EXAMEN

Sept enquêtes ont été choisies pour la vérification de cette année – cinq relevant de l'antiterrorisme et deux du contre-espionnage. Le Comité a examiné tous les dossiers et les documents électroniques ayant trait à chacune. Nous avons interviewé à la fois les gestionnaires de la région directement chargés des enquêtes et le personnel surveillant à l'Administration centrale.

CONSTATATIONS DU COMITÉ

D'après l'information examinée, le Comité est convaincu que, dans les sept cas, le Service avait des motifs raisonnables de soupçonner l'existence de menaces

envers la sécurité du Canada. Ni les dossiers et messages opérationnels que nous avons étudiés ni les entrevues que nous avons menées ne permettent de croire que les niveaux d'enquête étaient sans commune mesure avec les menaces présumées.

Nous avons aussi scruté les renseignements recueillis au cours des sept enquêtes. Dans un cas, nous avons demandé si certains renseignements étaient « strictement nécessaires ». En dépit des explications du Service, sa réponse ne nous a pas pleinement satisfaits. À notre avis, il n'était pas strictement nécessaire de recueillir ces renseignements et nous ne sommes pas convaincus que, dans ce cas-là, le Service s'est conformé en tout aux politiques et lignes directrices opérationnelles existantes en matière de collecte d'informations.

Gestion des enquêtes

Le Comité d'approbation et de réévaluation des cibles

Pour le SCRS, la possibilité de scruter les activités d'une personne, d'un groupe ou d'une organisation est soumise à des politiques qui comportent un contrôle rigoureux des méthodes et techniques employées à cet égard. Le Comité d'approbation et de révision des cibles (CARC) est au SCRS le principal groupe opérationnel qui est chargé d'étudier et d'approuver les demandes d'autorisation d'enquêter émanant des agents du Service. Il est présidé par le directeur du SCRS et composé de membres de la haute direction du Service et de représentants des ministères de la Justice et du Solliciteur général.

Niveaux d'enquête

Des trois niveaux d'enquête existants, le troisième est celui qui comporte le plus haut degré d'intrusion et que la loi et la haute direction soumettent aux mesures de contrôle les plus strictes. Les enquêtes de niveau 2 peuvent comprendre des entrevues personnelles et une filature limitée. Celles de niveau 1 ont une durée brève et permettent au SCRS de recueillir de l'information provenant de sources ouvertes et de dossiers conservés par des services étrangers de police, de sécurité ou de renseignement.

Enquêtes contextuelles

Une autorisation d'enquête contextuelle habilite le SCRS à enquêter sur les activités d'une personne, d'un groupe ou d'une organisation qu'il soupçonne, pour des motifs raisonnables, d'être une menace à l'égard de la sécurité du Canada et qui a un lien avec ce contexte ou secteur d'intérêt particulier ou qui en découle.

envers la sécurité du Canada. Ni les dossiers et messages opérationnels que nous avons étudiés ni les entrevues que nous avons menées ne permettent de croire que les niveaux d'enquête étaient sans commune mesure avec les menaces présumées.

Nous avons aussi scruté les renseignements recueillis au cours des sept enquêtes. Dans un cas, nous avons demandé si certains renseignements étaient « strictement nécessaires ». En dépit des explications du Service, sa réponse ne nous a pas pleinement satisfaits. À notre avis, il n'était pas strictement nécessaire de recueillir ces renseignements et nous ne sommes pas convaincus que, dans ce cas-là, le Service s'est conformé en tout aux politiques et lignes directrices opérationnelles existantes en matière de collecte d'informations.

Gestion des enquêtes

Le Comité d'approbation et de réévaluation des cibles

Pour le SCRS, la possibilité de scruter les activités d'une personne, d'un groupe ou d'une organisation est soumise à des politiques qui comportent un contrôle rigoureux des méthodes et techniques employées à cet égard. Le Comité d'approbation et de révision des cibles (CARC) est au SCRS le principal groupe opérationnel qui est chargé d'étudier et d'approuver les demandes d'autorisation d'enquêter émanant des agents du Service. Il est présidé par le directeur du SCRS et composé de membres de la haute direction du Service et de représentants des ministères de la Justice et du Solliciteur général.

Niveaux d'enquête

Des trois niveaux d'enquête existants, le troisième est celui qui comporte le plus haut degré d'intrusion et que la loi et la haute direction soumettent aux mesures de contrôle les plus strictes. Les enquêtes de niveau 2 peuvent comprendre des entrevues personnelles et une filature limitée. Celles de niveau 1 ont une durée brève et permettent au SCRS de recueillir de l'information provenant de sources ouvertes et de dossiers conservés par des services étrangers de police, de sécurité ou de renseignement.

Enquêtes contextuelles

Une autorisation d'enquête contextuelle habilite le SCRS à enquêter sur les activités d'une personne, d'un groupe ou d'une organisation qu'il soupçonne, pour des motifs raisonnables, d'être une menace à l'égard de la sécurité du Canada et qui a un lien avec ce contexte ou secteur d'intérêt particulier ou qui en découle.

Exécution des mandats

En vertu de l'article 21 de la Loi, seule la Cour fédérale du Canada peut, par la voie de mandats, octroyer au SCRS les pouvoirs l'habilitant à recourir aux méthodes d'enquête comportant le plus haut degré d'intrusion qui soit permis : l'interception de communications téléphoniques ou d'envois postaux. Chaque année, le Comité scrute l'exécution de mandats dans un certain nombre de dossiers choisis parmi ceux d'une région donnée.

Toutes les activités de collecte de renseignements sont conformes aux dispositions et conditions énoncées dans les mandats

Dans son examen, le Comité évalue :

- quel usage la Région fait des pouvoirs que la Cour fédérale lui octroie par la voie de mandats;
- si la Région respecte toutes les dispositions et conditions énoncées dans les mandats;
- si elle se conforme à la Loi, aux politiques du SCRS et aux instructions du Ministre dans l'exécution des mandats.

CONSTATATIONS DU COMITÉ

Exécution des mandats

L'examen des mandats sélectionnés par le Comité et des dossiers d'enquête pertinents n'a révélé aucun cas d'exercice inutile de pouvoirs conférés par mandat. Toutes les activités de collecte de renseignements sont conformes aux dispositions et conditions énoncées dans les mandats. Cependant, pour ce qui est des fruits de la collecte effectuée par le Service grâce à certains mandats et à ce qu'il en a conservé, le CSARS a relevé des anomalies possibles dans deux des cas examinés.

Dans le premier, le Comité a demandé au Service pourquoi il avait conservé des données d'un type particulier au-delà de la période normale prévue dans ses politiques opérationnelles. En réponse, le SCRS l'a informé qu'il avait autorisé la période spéciale de conservation afin de pouvoir aider un organisme allié dans son enquête sur un réseau terroriste.

Le second cas concerne l'interception de deux communications de personnes non désignées dans le mandat et les rapports à ce sujet. Le Comité est satisfait de

l'explication que le Service lui a donnée par la suite et selon laquelle, dans les deux circonstances où la chose semble s'être produite, les interceptions aient été légitimes et légales (l'une en vertu des dispositions de la clause « omnibus » et l'autre parce que la personne dont on a intercepté les communications s'apparentait à « Vanweenan[1] »).

Pénurie de personnel spécialisé

L'examen des dossiers d'enquête de la Région par le Comité montre que ce bureau manquait de spécialistes d'une certaine discipline. Même si les retards que cela occasionnait n'ont eu aucun effet néfaste sur les cas examinés, le CSARS voudrait éviter que les délais de traitement empêchent indûment de communiquer en temps opportun d'importants renseignements aux fonctionnaires compétents. Il a déjà exprimé des craintes semblables par le passé et il se réjouit des initiatives prises par le Service pour corriger la situation dans cette région.

Examen d'opérations délicates

Le recours aux sources humaines pour recueillir des informations est essentiel à l'efficacité des enquêtes sur les menaces à la sécurité publique et à la sûreté de l'État. Cependant, ces opérations sont tellement délicates qu'elles sont assujetties à des instructions spéciales du Ministre. De plus, les règles à suivre dans leur exécution sont exposées de façon assez détaillée dans le *Manuel des politiques sur les opérations* du SCRS. Toute demande visant une telle opération ou une enquête concernant des « institutions névralgiques » nécessite l'approbation de la haute direction du Service[2].

---

1. La clause omnibus permet d'intercepter les communications de personnes qui, même si elles ne sont pas nommées dans un mandat, peuvent se trouver en un endroit qui y est mentionné. La Cour suprême du Canada a confirmé la légalité de cette clause dans l'affaire *R c. Chesson*, [1988] 2 R.C.S. 148. Dans le même jugement, elle a confirmé la légalité de l'interception de communications d'une personne désignée ou décrite dans le mandat (à titre de « conjoint » ou de « collègue », par exemple) qui n'est pas ciblée de façon particulière, qui est susceptible d'avoir des rapports réguliers avec la cible et dont l'organisme chargé d'enquêter a des motifs raisonnables de croire que les communications pourraient lui faciliter la tâche. Depuis l'affaire « Chesson », le nom d'une des parties – Vanweenan – désigne cette catégorie de personnes.

2. La définition d'institution névralgique englobe les syndicats, les médias, les institutions religieuses ainsi que les campus universitaires et collégiaux.

MÉTHODE D'EXAMEN

Le Comité a examiné une série d'opérations choisies au hasard qui font appel à des sources humaines et toutes les demandes qui ont été présentées à la haute direction au sujet d'institutions névralgiques. Dans chaque cas, il a étudié tous les dossiers de recrutement, de mise à l'essai et d'exploitation des sources en question. Son but était de vérifier si, dans l'exploitation des sources et dans la conduite des enquêtes sur ces institutions, le Service s'était conformé à la Loi, aux instructions du Ministre et à ses propres politiques opérationnelles.

> Il y a eu infraction parce que les deux employés en cause avaient laissé leur véhicule hors de vue et sans surveillance

CONSTATATIONS DU COMITÉ

Pour ce qui est tant de la mise à l'essai et de l'exploitation des sources humaines par la Région que des enquêtes de celle-ci concernant des institutions névralgiques, le Comité a conclu que les actions du Service étaient légitimes, appropriées et nécessaires à la bonne exécution de son mandat.

Nous avons toutefois relevé un point où le Bureau régional n'avait pas respecté pleinement les politiques du Service relatives à certaines méthodes administratives. Le Comité est d'avis qu'une vérification périodique par la direction du Bureau aurait permis d'éviter cette lacune administrative.

Sécurité interne

VUE D'ENSEMBLE

Les recherches du Comité ont montré que le niveau de sensibilisation à la sécurité était généralement élevé au Bureau régional et que la direction avait pris les mesures voulues pour assurer la vigilance dans les rangs des employés du Service. Nous avons toutefois noté que la Région avait fouillé au hasard les porte-documents de ses employés sensiblement moins souvent que les autres bureaux régionaux du SCRS. Le Service nous a informés qu'en 2001–2002 le Bureau régional a pour objectif de fouiller les porte-documents chaque mois.

UNE INFRACTION À LA SÉCURITÉ

Le Comité a examiné les dossiers concernant une affaire d'infraction à la sécurité, survenue durant la période visée, qui a occasionné le vol de biens et de documents classifiés dans un véhicule opérationnel. Notre examen a révélé que le personnel de la sécurité interne de la Région et de l'Administration centrale du SCRS avait

mené une enquête efficace sur l'incident et que des correctifs appropriés avaient été apportés pour réduire les risques de voir se reproduire de semblables infractions à la sécurité.

Deux questions ont retenu l'attention du Comité dans cette affaire. Tout d'abord, il y a eu infraction parce que les deux employés en cause avaient laissé leur véhicule hors de vue et sans surveillance, ce qui était une erreur de jugement, à son avis. Ensuite, même si le Service a apporté des changements constructifs aux politiques et procédures en matière de sécurité à la suite de l'incident, certaines ambiguïtés évitables demeurent qui, de l'avis du CSARS, risquent d'affaiblir la politique dans son ensemble.

En réponse aux observations du Comité, le Service a affirmé que l'infraction ne découlait pas d'une erreur de jugement, que ses employés avaient pris toutes les précautions nécessaires et suivi toutes les procédures établies et, en outre, qu'aucune mesure disciplinaire n'était envisagée. Il a accepté de modifier son manuel des politiques afin de réduire les risques d'interprétation erronée.

C. Au sein du SCRS

Les mandats : généralités et données statistiques

Outre leur caractère extrêmement intrusif, les mandats sont l'un des instruments les plus puissants qui soient mis à la portée des ministères et organismes du gouvernement du Canada. C'est pour cette seule raison que leur utilisation doit être surveillée sans relâche et, cette tâche, le Comité la prend très au sérieux. De plus, en examinant l'usage que le Service fait des mandats, il peut saisir toute l'ampleur des activités d'enquête de celui-ci et il en tire un bon indicateur de la manière dont le SCRS conçoit ses priorités.

Le CSARS compile des statistiques trimestrielles sur tous les mandats décernés par la Cour fédérale et sur les affidavits qui sont joints aux demandes faites au tribunal. Il glane ainsi chaque année divers types de données, dont le nombre de personnes et de groupes que visent les pouvoirs conférés dans les mandats. Le tableau 1 fournit une comparaison du nombre de mandats qui ont été décernés au cours des trois derniers exercices financiers.

La Cour fédérale a décerné 32 mandats urgents en 2000–2001. Elle n'a rejeté aucune demande de mandat au cours de cet exercice et aucune de ses décisions n'a eu d'incidences sur les pouvoirs conférés dans des mandats existants.

DONNÉES SUR LES MANDATS

Les chiffres recueillis par le Comité fournissent une bonne idée de la manière dont le Service exerce les pouvoirs qui lui sont conférés par mandat durant un exercice donné, mais leur comparaison une année sur l'autre est plus problématique. Tout un éventail de facteurs, aussi disparates que les décisions judiciaires et les progrès technologiques, amène de profondes variations dans la manière dont se font les demandes de mandats et dans l'exécution de ceux-ci. Même les données brutes concernant les mandats peuvent être trompeuses, car un seul de ces documents peut autoriser l'exercice de pouvoirs contre plus d'une personne.

Compte tenu de ces facteurs, le Comité est toutefois en mesure de conclure que, depuis trois ans, le nombre total de personnes touchées par les pouvoirs octroyés au SCRS au moyen de mandats est demeuré relativement stable et que la majorité d'entre elles sont encore des ressortissants étrangers.

RÈGLEMENTS

Selon l'article 28 de la *Loi sur le SCRS*, le gouverneur en conseil peut prendre des règlements prescrivant la marche à suivre par le Service pour obtenir des mandats. En 2000–2001, il n'y a eu aucun règlement semblable.

---

3. Un mandat de remplacement est nécessaire si le Service change les cibles, les endroits ou les pouvoirs prévus dans un mandat existant.

Les organes opérationnels du SCRS

LE CONTRE-ESPIONNAGE

La Direction du contre-espionnage (CE) s'occupe des menaces qui peuvent peser sur la sécurité nationale en raison des activités d'espionnage menées au Canada par les services de renseignement de gouvernements étrangers.

Durant l'exercice visé, le Service a réaffecté à l'interne des ressources humaines et autres afin de pouvoir relever les défis, à son avis de plus en plus complexes, que suscitent deux secteurs du mandat de la Direction du CE : la lutte contre la prolifération et la criminalité transnationale. Tout comme d'autres directions du Service, le Contre-espionnage estime prioritaire de recruter et de maintenir en poste des employés qui connaissent à fond l'informatique et d'autres sciences, les marchés financiers internationaux et divers domaines techniques spécialisés. Le CE s'est enrichi de certaines spécialités grâce au détachement d'employés de ministères.

Le Service dit avoir réussi à enrayer au Canada les activités d'un certain nombre de services de renseignement étrangers en poursuivant ses efforts pour nouer des rapports de liaison constructifs. Il a en outre cité plusieurs cas de coopération

Rôle du SCRS dans la prévention de la violence à caractère politique

Le SCRS joue un rôle central dans la défense du Canada contre les menaces que peuvent représenter les groupes associés à la violence à caractère politique. Au nombre des « menaces envers la sécurité du Canada » sur lesquelles il est expressément chargé d'enquêter figurent « les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique au Canada ou dans un État étranger » (alinéa c) de la définition de menaces, article 2 de la *Loi sur le SCRS*).

Outre le fait qu'il informe l'ensemble du gouvernement sur la nature des menaces envers la sécurité du Canada, le SCRS prodigue renseignements et conseils directement à plusieurs ministères et organismes gouvernementaux. Cette information peut fonder les profils destinés au filtrage des immigrants. Dans certains cas, les conseils du SCRS peuvent être déterminants dans l'admission d'un demandeur ou dans le rejet d'une demande de citoyenneté. Les renseignements de sécurité peuvent aussi servir à déterminer s'il convient d'autoriser l'accès d'un individu à des renseignements classifiés, ainsi qu'à seconder la police dans son rôle en matière de prévention du crime et de poursuites au criminel.

Tableau 1
Mandats nouveaux et remplacees

	1998–1999	1999–2000	2000–2001
Nouveaux mandats	84	76	56
Mandats nouveaux et remplacés[1]	163	181	150
Total	247	257	206

La Cour fédérale a décerné 32 mandats urgents en 2000–2001. Elle n'a rejeté aucune demande de mandat au cours de cet exercice et aucune de ses décisions n'a eu d'incidences sur les pouvoirs conférés dans des mandats existants.

DONNÉES SUR LES MANDATS

Les chiffres recueillis par le Comité fournissent une bonne idée de la manière dont le Service exerce les pouvoirs qui lui sont conférés par mandat durant un exercice donné; mais leur comparaison une année sur l'autre est plus problématique. Tout un éventail de facteurs, aussi disparates que les décisions judiciaires et les progrès technologiques, amène de profondes variations dans la manière dont se font les demandes de mandats et dans l'exécution de ceux-ci. Même les données brutes concernant les mandats peuvent être trompeuses, car un seul de ces documents peut autoriser l'exercice de pouvoirs contre plus d'une personne.

Compte tenu de ces facteurs, le Comité est toutefois en mesure de conclure que, depuis trois ans, le nombre total de personnes touchées par les pouvoirs octroyés au SCRS au moyen de mandats est demeuré relativement stable et que la majorité d'entre elles sont encore des ressortissants étrangers.

RÈGLEMENTS

Selon l'article 28 de la *Loi sur le SCRS*, le gouverneur en conseil peut prendre des règlements prescrivant la marche à suivre par le Service pour obtenir des mandats. En 2000–2001, il n'y a eu aucun règlement semblable.

[1] Les mandats de remplacement visent à remplacer ou à modifier les mandats en vigueur lorsque les cibles, les activités ou les pouvoirs prévus dans un mandat changent.

Les organes opérationnels du SCRS

LE CONTRE-ESPIONNAGE

La Direction du contre-espionnage (CE) s'occupe des menaces qui peuvent peser sur la sécurité nationale en raison des activités d'espionnage menées au Canada par les services de renseignement de gouvernements étrangers.

Durant l'exercice visé, le Service a réaffecté à l'interne des ressources humaines et autres afin de pouvoir relever les défis, à son avis de plus en plus complexes, que suscitent deux secteurs du mandat de la Direction du CE : la lutte contre la prolifération et la criminalité transnationale. Tout comme d'autres directions du Service, le Contre-espionnage estime prioritaire de recruter et de maintenir en poste des employés qui connaissent à fond l'informatique et d'autres sciences, les marchés financiers internationaux et divers domaines techniques spécialisés. Le CE s'est enrichi de certaines spécialités grâce au détachement d'employés de ministères.

Le Service dit avoir réussi à enrayer au Canada les activités d'un certain nombre de services de renseignement étrangers en poursuivant ses efforts pour nouer des rapports de liaison constructifs. Il a en outre cité plusieurs cas de coopération

Rôle du SCRS dans la prévention de la violence à caractère politique

Le SCRS joue un rôle central dans la défense du Canada contre les menaces que peuvent représenter les groupes associés à la violence à caractère politique. Au nombre des « menaces envers la sécurité du Canada » sur lesquelles il est expressément chargé d'enquêter figurent « les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique au Canada ou dans un État étranger » (alinéa c) de la définition de menaces, article 2 de la *Loi sur le SCRS*).

Outre le fait qu'il informe l'ensemble du gouvernement sur la nature des menaces envers la sécurité du Canada, le SCRS prodigue renseignements et conseils directement à plusieurs ministères et organismes gouvernementaux. Cette information peut fonder les profils destinés au filtrage des immigrants. Dans certains cas, les conseils du SCRS peuvent être déterminants dans l'admission d'un demandeur ou dans le rejet d'une demande de citoyenneté. Les renseignements de sécurité peuvent aussi servir à déterminer s'il convient d'autoriser l'accès d'un individu à des renseignements classifiés, ainsi qu'à seconder la police dans son rôle en matière de prévention du crime et de poursuites au criminel.

fructueuse avec des organismes canadiens et des services de renseignement étrangers de pays alliés.

L'ANTITERRORISME

La Direction de l'antiterrorisme (AT) a pour rôle de conseiller le gouvernement au sujet des nouvelles menaces de violence grave qui pourraient compromettre la sécurité des Canadiens et de leurs alliés et la sûreté de leurs pays. Faire échec à la violence grave à caractère politique, d'origine intérieure ou étrangère, demeure l'une des grandes priorités du Service.

En 2000–2001, la Direction de l'AT a modifié son organisation et sa structure afin de suivre l'évolution de la menace terroriste. Le Service estime que l'une de ses principales difficultés dans la lutte contre le terrorisme est le recours de plus en plus fréquent aux technologies de pointe par les extrémistes pour mener, soutenir et dissimuler leurs opérations.

Les évaluations de menaces

Le SCRS fournit des évaluations de menaces aux ministères et organismes fédéraux en se fondant sur des renseignements pertinents et à propos. Ces évaluations – qui ont trait aux événements spéciaux, aux menaces pesant sur des institutions diplomatiques au Canada et à diverses situations, – il les effectue sur demande ou de sa propre initiative. Elles peuvent jouer un rôle crucial, non seulement pour informer les autorités si une activité telle une manifestation risque de devenir violente, mais aussi pour les rassurer quant aux situations où les risques de violence sont négligeables.

En 2000–2001, la Sous-section de l'évaluation de la menace a fait 544 évaluations en tout, soit un peu plus que durant l'exercice précédent. Ce total, le Comité en est conscient, dépend de divers facteurs qui sont indépendants de la volonté du Service : nombre de visiteurs étrangers au Canada, demandes des ministères et organismes, événements spéciaux et menaces relevées au cours de l'exercice.

L'EAP (EXIGENCES, ANALYSE ET PRODUCTION)

À titre d'organe de recherche du SCRS, la Direction des exigences, de l'analyse et de la production fournit au gouvernement des avis sur les menaces qui peuvent peser sur la sécurité du pays en rédigeant les *Rapports du SCRS*, les *Études du SCRS* et les *Bulletins de renseignements*. De plus, à partir de renseignements de source ouverte, elle publie deux séries de rapports non classifiés, intitulés *Perspectives* et *Commentaires*, qui revêtent un intérêt en matière de sécurité pour la collectivité du renseignement et pour le public.

En 2000–2001, l'EAP a produit 93 rapports, soit près du double de l'exercice précédent, ce qui est un revirement par rapport à la tendance à la baisse des dernières années. Ses publications entrent généralement dans deux catégories :

- les rapports sur la sécurité publique, qui traitent des menaces que le terrorisme international fait peser sur les Canadiens au pays ou à l'étranger; et
- les rapports ayant trait à la sûreté nationale qui portent sur les activités au Canada de services de renseignement d'autres gouvernements nationaux et sur des dossiers internationaux tels la lutte contre la prolifération et les activités criminelles transnationales.

L'apport du SCRS à l'ensemble de la collectivité gouvernementale du renseignement se traduit en outre par sa participation au Comité d'évaluation du renseignement (CER), qui se compose de hauts fonctionnaires des ministères et organismes fédéraux qui s'intéressent au premier chef aux questions liées au renseignement. Durant l'exercice à l'étude, le personnel de l'EAP a contribué à huit des rapports du CER, qui sont distribués au personnel supérieur de l'ensemble de l'administration gouvernementale.

Dans son rapport de 1998–1999, le CSARS avait recommandé de rétablir le Comité principal de production de renseignements (CPPR), organe interne du SCRS créé en 1987 (qui ne se réunissait cependant plus), de sorte que la production du renseignement réponde aux besoins de l'ensemble des clients ministériels du Service. Depuis, celui-ci a décidé d'abandonner le cycle de planification annuel qu'il avait envisagé initialement pour ce comité et, plutôt, d'examiner plus souvent les activités de production de renseignements de l'EAP et d'en rendre compte comme il se doit aux cadres supérieurs compétents du Service. À l'avenir, des réunions officielles du CPPR seront tenues au besoin seulement.

Ententes avec les ministères et les gouvernements

RELATIONS AVEC LA GRC

Les mécanismes de liaison et de coopération entre le Service et la GRC sont prévus dans le protocole d'entente que ceux-ci ont conclu. La coopération est facilitée par l'affectation réciproque d'agents de liaison aux administrations centrales nationales et dans tous les bureaux régionaux des deux organismes.

Pour l'exercice à l'étude, le Service a fait état de plusieurs initiatives nouvelles visant à améliorer la coopération avec la GRC :

- un programme d'échange de personnel entre les administrations centrales nationales, avec un accent particulier sur la criminalité transnationale;
- des échanges de personnel et des ententes entre plusieurs bureaux régionaux en vue d'autres échanges; et
- la tenue par le SCRS, au niveau régional, de « journées portes ouvertes » à la GRC et aux autres services de police.

Le SCRS et la GRC échangent couramment des informations sur les activités entourant leurs mandats respectifs. Le Service recueille et communique des renseignements au sujet des menaces à la sécurité du Canada et la GRC exerce les fonctions d'exécution de la loi que lui confère son mandat relativement aux mêmes menaces. Au cours de l'exercice 2000–2001, les deux organismes ont échangé 1 678 documents dont le SCRS a été appelé à fournir plus de la moitié (949). Le Service a en outre remis à la GRC 330 notes de communication[4] et 39 lettres d'autorisation[5].

ENTENTES AVEC DES ORGANISMES CANADIENS

Dans l'exécution de son mandat, le Service coopère avec les services de police et avec les ministères et organismes fédéraux et provinciaux de l'ensemble du Canada. L'alinéa 17(1)a) de la Loi l'habilite à conclure par écrit des ententes de coopération avec des organismes canadiens, moyennant autorisation du Ministre.

Actuellement, le SCRS a dix-neuf protocoles d'entente officiels avec des ministères et organismes fédéraux et huit avec des organismes provinciaux. Il a en outre un accord distinct avec plusieurs services de police d'une province.

En 2000–2001, le Service a conclu avec un organisme provincial une entente pour la prestation d'évaluations de sécurité et il a demandé au Ministre l'autorisation d'en conclure une seconde pour la liaison avec un autre organisme. Aucune entente existante n'a été modifiée ou abrogée.

---

4. À la suite d'une demande officielle de la GRC, le SCRS communique des informations ou renseignements sous une forme qui protège l'identité des sources et les méthodes employées pour recueillir l'information. La communication est assujettie à la condition que l'information serve uniquement de piste dans des enquêtes, et non dans des instances judiciaires.

5. À la suite d'une demande officielle de la GRC – soit généralement après une communication – le SCRS autorise la GRC, au moyen d'une lettre, à utiliser ses renseignements dans des instances judiciaires, par exemple, à l'occasion de demandes de mandat ou à titre de preuve dans des procès.

ENTENTES AVEC DES ORGANISMES ÉTRANGERS

Avant de conclure une entente avec le gouvernement d'un État étranger ou avec une organisation internationale, le Service doit, aux termes de l'alinéa 17(1)b) de la *Loi sur le SCRS*, obtenir l'approbation du solliciteur général qui consulte alors le ministre des Affaires étrangères et du Commerce international. Pendant les démarches initiales menant à l'approbation d'une telle entente, le SCRS ne peut communiquer de renseignements classifiés à l'entité intéressée, mais il peut en accepter ceux qu'elle lui fournit spontanément.

Au cours de l'exercice 2000–2001, le Ministre a autorisé le Service à conclure cinq nouvelles ententes de liaison. Parmi les ententes actuellement en vigueur, le SCRS estime que 44 sont « inappliquées[6] ». Six d'entre elles ont été modifiées de manière à élargir l'éventail des informations échangées et une autre, qui était inappliquée, a été réactivée pour faciliter les activités du Service liées au filtrage de sécurité et à l'immigration dans le pays en cause.

Aucune entente de liaison en place n'a été annulée. Le Service a toutefois réduit le niveau des échanges avec deux organismes étrangers : en raison de craintes liées aux droits de la personne dans un cas et, dans l'autre, à cause d'une évaluation qui mettait en doute la fiabilité et la stabilité de l'organisme concerné.

BUREAUX D'AGENT DE LIAISON-SÉCURITÉ

Dans bien des pays, le Service a des bureaux d'agent de liaison-sécurité (ALS) qui sont chargés d'assurer les relations avec les services de police, de sécurité et de renseignement. Les autorités de ces États sont au courant de la présence des agents et en connaissent les fonctions, condition sine qua non de la coopération mutuelle. Le nombre de ces bureaux à l'étranger était le même qu'au cours de l'exercice précédent.

La collecte de renseignements étrangers

L'article 16 de la *Loi sur le SCRS* habilite le Service à recueillir des renseignements étrangers à la demande écrite du ministre des Affaires étrangères et du Commerce international ou du ministre de la Défense nationale et avec l'approbation écrite

6. Une entente est dite inappliquée si elle n'a donné lieu à aucun contact durant une année ou plus. Cette non-application peut tenir à divers facteurs, dont la simple absence de besoin d'échanger des informations, les craintes du Service quant aux usages professionnels ou au respect des droits de la personne par l'autre organisme ou le fait que la situation politique est jugée trop instable dans l'autre pays.

du solliciteur général. La Loi autorise le SCRS à demander des mandats pour obtenir divers pouvoirs, dont celui d'intercepter des communications téléphoniques, et à entreprendre d'autres activités d'enquête à la demande de ces ministres.

Le terme renseignements étrangers désigne les informations ou renseignements concernant les « moyens, les intentions ou les activités » d'un État étranger. D'après la *Loi sur le SCRS*, la collecte de tels renseignements par le Service doit se faire au Canada et ne peut viser des citoyens, des résidents permanents ou des entreprises du pays.

MÉTHODE D'EXAMEN

L'examen effectué par le Comité englobe toutes les « demandes d'assistance » émanant de ministres, tous les renseignements conservés par le SCRS sur le compte de Canadiens pour les besoins de la sécurité nationale et tous les échanges d'informations avec le Centre de la sécurité des télécommunications (CST) dans le contexte du renseignement étranger.

Le terme renseignements étrangers désigne les informations ou renseignements concernant les « moyens, les intentions ou les activités » d'un État étranger

Le CST – organisme qui relève du ministère de la Défense nationale – fournit au gouvernement du Canada, au sujet de pays étrangers, les renseignements électromagnétiques (SIGINT) qu'il obtient en recueillant et en analysant leurs transmissions par radio, par radar et par d'autres moyens électroniques, parfois en collaboration avec les organismes de pays alliés.

L'objectif de l'examen est le suivant :

- vérifier si le rôle du Service à l'égard des demandes présentées en vertu de l'article 16 est conforme à la *Loi sur le SCRS*, aux directives de la Cour fédérale et au protocole d'entente applicable (1987) entre le ministre des Affaires étrangères et du Commerce international, celui de la Défense nationale et le solliciteur général;
- déterminer si le Service a respecté les diverses conditions prescrites par la loi pour la collecte de renseignements dans le cadre d'opérations relevant de l'article 16; et

- examiner la nature de la coopération du SCRS avec le CST afin de déterminer si celle-ci est irréprochable et conforme à la loi.

CONSTATATIONS DU COMITÉ

Exécution des mandats

Comme les activités de collecte de renseignements en vertu de l'article 16 nécessitent toutes un mandat de la Cour fédérale, le Service est tenu d'observer les diverses conditions et restrictions qui y sont rattachées. Le Comité a examiné un échantillon de mandats obtenus à cette fin ainsi que les affidavits et dossiers généraux pertinents. Dans les dossiers examinés, les mandats ont été exécutés dans les règles et les conditions pertinentes, respectées.

Demandes de renseignements au CST

Comme il est interdit de recueillir des renseignements sur les ressortissants et entreprises du Canada, le CST assujettit couramment l'information qu'il communique au SCRS au principe de la « divulgation minimale ». Ainsi, s'il obtient indirectement le nom d'un Canadien membre du milieu des affaires, il tait ce nom en y substituant l'expression « un entrepreneur canadien ». Dans des circonstances particulières, le Service peut demander au CST de lui révéler l'identité de l'intéressé s'il peut faire la preuve que ce renseignement a trait à des activités qui pourraient constituer une menace envers la sécurité du Canada, au sens de l'article 2 de la *Loi sur le SCRS*.

Dans le cadre de ses vérifications, le Comité a examiné si les demandes présentées au CST étaient légitimes et conformes aux lois et politiques existantes. Il en a trouvé trois qui ne semblaient pas répondre aux critères énoncés à l'article 2 de la Loi.

L'une des demandes concernait un Canadien en vue qu'avait approché un ressortissant étranger et une autre visait une institution névralgique (syndicat, groupe médiatique, organisme religieux ou campus universitaire) qui avait pris part à des campagnes politiques dans un pays étranger. Le Service nous a informés que, dans les deux cas, l'information recueillie avait été retirée de ses dossiers à la suite de notre examen.

Dans le troisième cas, le Service avait conservé dans ses dossiers des listes de personnes qui avaient pris part à plusieurs réunions mondaines avec des ressortissants

étrangers. Le SCRS a effectué des vérifications de dossiers dans le cas de certaines de ces personnes.

Le Comité a demandé au Service pourquoi il avait conservé ces listes, affirmant que cela ne lui semblait pas « strictement nécessaire », contrairement à ce que prescrit la Loi. Le SCRS a répondu que c'était parce que les intéressés avaient eu des rapports avec une cible déjà visée par une enquête en vertu de l'article 12. Sa réponse a satisfait le CSARS.

Section 2

Filtrage de sécurité et enquêtes sur les plaintes

Filtrage de sécurité et enquêtes sur les plaintes

La *Loi sur le SCRS* confère au Comité le double mandat d'examiner toutes les activités du Service et d'étudier les plaintes à cet égard. La présente section du rapport annuel porte sur la seconde de ces responsabilités principales du CSARS. De plus, comme une certaine proportion des plaintes a trait aux fonctions du Service en matière de filtrage de sécurité, notre examen relatif à ce volet de son mandat fournit le contexte dont nous aurons besoin pour nous pencher ensuite sur les plaintes.

A. Filtrage de sécurité

En vertu du paragraphe 13(1) de la *Loi sur le SCRS*, le Service est habilité à fournir des évaluations de sécurité aux ministères fédéraux. Moyennant l'approbation ministérielle voulue, il peut aussi conclure des ententes pour la prestation de telles évaluations, selon le paragraphe 13(2), avec les ministères ou les services de police provinciaux. Les ententes visant les évaluations de sécurité destinées aux gouvernements ou organismes d'États étrangers et aux institutions et organisations internationales sont autorisées au paragraphe 13(3).

En ce qui touche l'emploi dans la fonction publique fédérale, les évaluations de sécurité du SCRS servent à déterminer s'il y a lieu d'autoriser les intéressés à avoir accès à des renseignements ou à des biens classifiés. Dans les dossiers d'immigration, les évaluations du Service peuvent être déterminantes pour Citoyenneté et Immigration Canada qui doit trancher s'il y a lieu d'admettre des personnes au pays et d'octroyer le statut de résident permanent ou la citoyenneté.

ÉVALUATIONS DE SÉCURITÉ POUR LE GOUVERNEMENT FÉDÉRAL

Principales statistiques pour 2000-2001

- Le Service a reçu 36 803 demandes d'évaluation de sécurité en vue d'habilitations de niveaux I, II et III, tant nouvelles que rehaussées ou mises à jour, mais surtout de niveau II. En outre, 418 demandes visaient des mesures administratives, tels des transferts et des abaissements d'habilitations.
- Pour les habilitations de sécurité de niveaux I, II et III, le temps de traitement moyen a été de 32 jours, 41 jours et 113 jours, respectivement.

Le filtrage de sécurité dans l'administration fédérale

La Politique fédérale sur la sécurité prévoit deux types d'enquêtes de sécurité du personnel : une évaluation de fiabilité et une évaluation de sécurité. Ces évaluations font partie des conditions d'emploi prévues dans la *Loi sur l'emploi dans la fonction publique*.

Cote de fiabilité de base

Chaque ministère et organisme fédéral a la responsabilité de décider quel type d'enquête de sécurité est nécessaire. Cette décision dépend de la nature délicate des renseignements et des biens auxquels l'intéressé devra avoir accès. Le niveau « minimum » d'enquête est exigé pour les personnes qui sont nommées ou affectées à un poste pour six mois ou plus dans la fonction publique, et pour celles que la fonction publique fédérale engage à contrat pour plus de six mois et qui doivent avoir accès régulièrement aux installations de l'État. Les personnes qui obtiennent cette cote peuvent avoir accès uniquement à des renseignements de nature non délicate (c.-à-d. non classifiés ou non désignés).

Cote de fiabilité approfondie

Une cote de fiabilité approfondie est exigée quand les fonctions d'un poste de fonctionnaire fédéral ou d'un contrat nécessitent un accès fréquent aux renseignements ou biens classifiés de l'État, quelle que soit la durée de l'affectation. Les personnes qui obtiennent cette cote peuvent avoir accès, au besoin, à des renseignements et biens désignés.

Les ministères et organismes fédéraux ont la responsabilité de déterminer quelles vérifications sont nécessaires quant aux données personnelles, aux études ou aux titres et qualités professionnels ainsi qu'aux données sur l'emploi. Ils peuvent aussi décider de faire une vérification nominale du casier judiciaire.

Lorsqu'ils font des évaluations de fiabilité, les organismes fédéraux sont tenus de porter des jugements justes et objectifs qui respectent les droits des intéressés. D'après la Politique sur la sécurité, « les personnes visées doivent avoir l'occasion d'expliquer les renseignements défavorables avant qu'une décision ne soit prise, et il faut leur donner les motifs du refus d'une cote de fiabilité, à moins que ces renseignements ne fassent l'objet d'une exception en vertu de la *Loi sur la protection des renseignements personnels* ».

Les évaluations de sécurité

Au sens de la *Loi sur le SCRS*, l'évaluation de sécurité est un jugement porté sur la loyauté d'un individu envers le Canada et, à cet égard, sur sa fiabilité. Avant de demander une évaluation de sécurité, le ministère ou organisme gouvernemental compétent doit autoriser une cote de fiabilité « de base » ou « approfondie ». Même si elle a obtenu cette cote administrativement, une personne ne peut être nommée à un poste donnant accès à des renseignements ou biens classifiés tant que la cote de sécurité ne lui a pas été attribuée.

- La majeure partie des 3 670 enquêtes locales ont été requises par le ministère de la Défense nationale, suivi du SCRS, du ministère des Affaires étrangères et du Commerce international, du Centre de la sécurité des télécommunications et du ministère des Travaux publics et des Services gouvernementaux.
- Le Service a reçu 37 128 demandes d'évaluation pour le Programme d'autorisation d'accès aux zones réglementées d'aéroports, qui relève de Transports Canada. Le temps de traitement moyen de ces demandes a été de 32 jours, sensiblement plus que l'an dernier, soit 4 jours. Le SCRS a expliqué cet écart par le volume élevé des demandes d'évaluation de sécurité et par l'arriéré qui en avait résulté.
- Il y a eu 1 439 demandes d'évaluation de sécurité pour autorisation d'« accès à des sites ». Pour ces évaluations, on procède à une vérification de base de la fiabilité des intéressés avant d'autoriser l'accès à des sites névralgiques.
- De concert avec la GRC agissant à titre d'intermédiaire, le Service a traité 268 demandes d'autorisation d'accès à la Cité parlementaire et 11 129 demandes d'accréditation à des rencontres et activités spéciales auxquelles l'accès est contrôlé.

PROGRAMMES DE FILTRAGE DE SÉCURITÉ À L'IMMIGRATION

En vertu des articles 14 et 15 de la *Loi sur le SCRS*, le Service effectue des enquêtes de sécurité et fournit des conseils au ministre de la Citoyenneté et de l'Immigration (CIC). En règle générale, son assistance sur ce plan va des échanges d'informations sur les questions entourant les menaces à la sécurité du Canada, au sens de l'article 2 de la *Loi sur le SCRS*, aux « évaluations » concernant les catégories de personnes non admissibles en vertu de l'article 19 de la *Loi sur l'immigration*.

Demandes de résidence permanente présentées au Canada

Le Service a la responsabilité exclusive de filtrer les demandes de résidence permanente présentées au Canada par les immigrants et les réfugiés. En 2000–2001, il en a reçu 44 278[7]. Le temps de traitement moyen de ces demandes a été de 66 jours, soit 195 pour les demandes écrites et 60 pour celles présentées par voie électronique.

Demandes de résidence permanente provenant de l'étranger

Les demandes de résidence permanente provenant d'autres pays que le Canada et les États-Unis relèvent du Programme de filtrage des demandes d'immigration

7. Ce chiffre comprend 4 217 demandes de filtrage de sécurité provenant des États-Unis et traitées au Canada.

à l'étranger. En vertu de ce programme, le SCRS partage la responsabilité du filtrage de sécurité avec les fonctionnaires de CIC en poste dans ces autres pays. En règle générale, il ne prend part à ce processus que si le gestionnaire du Programme d'immigration l'y invite ou s'il reçoit des renseignements défavorables d'informateurs confirmés. Cette répartition des tâches permet au Service de se concentrer sur les dossiers présentant le plus de risques.

Les délais de traitement des demandes ont été sensiblement plus longs que les années antérieures

En 2000–2001, le Service a reçu 25 109 demandes de l'étranger. À cet égard, il a signalé que les gestionnaires du Programme d'immigration avaient consulté ses agents de liaison-sécurité (ALS) au sujet de 4 433 dossiers entre le 1er avril et le 31 décembre 2000.

Nature des conseils du Service à CIC

Les demandes de filtrage de sécurité liées à l'immigration ont donné lieu à 216 notes du SCRS à CIC – 167 avis de non-admissibilité et 49 notes d'information. Pour la période à l'étude, il a fallu au Service environ un an et demi en moyenne pour traiter une demande. Le SCRS a envoyé 90 « lettres d'anecdote » et 61 lettres de mise à jour à CIC. (Voir à la page 13 la description des notes, avis et autres documents d'information employés par le Service pour seconder les programmes d'immigration du Canada.)

Filtrage de sécurité : délais de traitement accrus

Dans l'ensemble, les délais de traitement des demandes de CIC par le SCRS ont été sensiblement plus longs que les années antérieures. Pour expliquer la chose, le Service a cité deux facteurs principaux, tous deux temporaires, à son avis. Le premier est un important arriéré de demandes, reçues de l'étranger sur « papier », qui sont passablement plus longues à traiter que celles présentées au Canada par voie électronique. Le SCRS a assuré au Comité que l'arriéré avait été éliminé et qu'il avait pris des mesures pour éviter toute nouvelle accumulation de demandes. Par ailleurs, les problèmes liés à la mise en œuvre de nouveaux logiciels au cours de l'exercice, combinés aux ajustements requis pour faire face au bogue de l'an 2000, ont occasionné d'autres retards. Ces problèmes sont en voie d'être réglés.

Les demandes de citoyenneté et la Liste de surveillance

Dans le cadre du processus de filtrage des demandes de citoyenneté, le Service reçoit par voie électronique les demandes de vérification de dossiers du Centre de traitement des données de Sydney, en Nouvelle-Écosse. Il vérifie si les noms des intéressés figurent dans la base de données du Système d'information sur le

filtrage de sécurité. La Liste de surveillance que tient le SCRS contient les noms d'individus qui ont été portés à son attention, entre autres au cours d'enquêtes approuvées par le CARC, et qui ont obtenu le statut d'immigrant reçu.

En 2000–2001, le Service a reçu 161 895 demandes de citoyenneté. Il a recommandé le rejet dans quatre cas et rédigé des notes d'information relativement à 78 autres. Dans un cas, il a demandé au Ministre l'autorisation de reporter la présentation de son évaluation[8].

Nouveau programme : filtrage des réfugiés

Comme le mentionne le Comité dans l'étude des notes de filtrage de sécurité à l'immigration (voir page 13), le Service et CIC ont conclu récemment l'entente « Filtrage dès le début du processus », des demandeurs du statut de réfugié. Ce projet pilote consistera initialement à installer du matériel d'échange électronique d'informations dans cinq bureaux de CIC au Canada.

ÉVALUATIONS DE SÉCURITÉ POUR LES ORGANISMES ÉTRANGERS

Le Service peut conclure avec des organismes étrangers des ententes visant la prestation réciproque de vérifications de sécurité concernant des Canadiens et d'autres personnes qui ont habité au Canada. Au cours de la période considérée, le SCRS a effectué, pour le compte de tels organismes, 995 évaluations de sécurité dont 66 ont nécessité des enquêtes sur place. Celles-ci l'ont amené à envoyer une note d'information à son client.

B. Enquêtes sur les plaintes

Outre ses fonctions de surveillance et d'examen, le Comité a charge d'enquêter sur les plaintes du public au sujet de toute action du SCRS. À cet égard, trois types de plaintes ressortissent au CSARS :

- À titre de tribunal quasi judiciaire, le Comité est autorisé à examiner toute affaire ayant trait aux habilitations de sécurité demandées par le gouvernement fédéral, y compris les plaintes à l'égard du refus d'habilitations à des fonctionnaires ou à des fournisseurs de l'État, et à faire rapport à ce sujet.

8. S'il estime ne pas être en mesure de faire de recommandation à CIC à l'égard d'une demande de citoyenneté, le Service doit requérir du solliciteur général l'autorisation de poursuivre son enquête à ce sujet et de « reporter » la présentation de son évaluation.

- Le CSARS peut faire enquête sur les rapports de ministres à l'endroit de personnes relativement à des affaires de citoyenneté et d'immigration, à certains dossiers touchant les droits de la personne et au crime organisé.
- Comme le prescrit la *Loi sur le SCRS*, le Comité reçoit en tout temps les plaintes qui peuvent être portées « contre des activités du Service ».

CONSTATATIONS AU SUJET DES PLAINTES RELEVANT DE L'ARTICLE 41 – « ACTIVITÉS »

Au cours de 2000–2001, le Comité a examiné 69 plaintes portées en vertu de l'article 41 de la *Loi sur le SCRS*, dont 52 nouvelles et 17 reportées de l'exercice précédent.

Plaintes relatives à des affaires d'immigration

Dans le droit fil de la tendance observée ces dernières années, une forte proportion des plaintes présentées au Comité en 2000–2001 – soit 34 en tout – ont trait au rôle joué par le Service dans le programme d'immigration du Canada.

Plaintes concernant des actes répréhensibles et des abus de pouvoir

Durant la période à l'étude, le Comité a examiné 20 plaintes dont les auteurs prétendaient que le Service les avait placés sous surveillance, avait posé à leur endroit des gestes illégaux ou avait autrement abusé de ses pouvoirs.

Tableau 2
Plaintes (du 1er avril 2000 au 31 mars 2001)

	Nouvelles plaintes	Plaintes reportées de 1999–2000	Réglées en 2000–2001	Reportées à 2000–2001
Activités du SCRS	52	17	30	39
Habilitations de sécurité	0	4	2	2
Immigration	0	1	1	0
Citoyenneté	0	1	1	0
Droits de la personne	0	1	1	0

- Le CSARS peut faire enquête sur les rapports de ministres à l'endroit de personnes relativement à des affaires de citoyenneté et d'immigration, à certains dossiers touchant les droits de la personne et au crime organisé.
- Comme le prescrit la *Loi sur le SCRS*, le Comité reçoit en tout temps les plaintes qui peuvent être portées « contre des activités du Service ».

CONSTATATIONS AU SUJET DES PLAINTES RELEVANT DE L'ARTICLE 41 – « ACTIVITÉS »

Au cours de 2000–2001, le Comité a examiné 69 plaintes portées en vertu de l'article 41 de la *Loi sur le SCRS*, dont 52 nouvelles et 17 reportées de l'exercice précédent.

Plaintes relatives à des affaires d'immigration

Dans le droit fil de la tendance observée ces dernières années, une forte proportion des plaintes présentées au Comité en 2000–2001 – soit 34 en tout – ont trait au rôle joué par le Service dans le programme d'immigration du Canada.

Plaintes concernant des actes répréhensibles et des abus de pouvoir

Durant la période à l'étude, le Comité a examiné 20 plaintes dont les auteurs prétendaient que le Service les avait placés sous surveillance, avait posé à leur endroit des gestes illégaux ou avait autrement abusé de ses pouvoirs.

Pour ne pas révéler indirectement à quelles cibles s'intéresse le Service, le Comité ne confirme pas ni n'infirme, en principe, si les plaignants sont visés par des autorisations d'enquête du SCRS. Même s'il ne leur fournit pas cette information, il procède à des investigations poussées sur leurs allégations.

Dans ses investigations, le Comité s'assure que les activités du Service ont été menées conformément à la Loi, aux instructions du Ministre et aux politiques du SCRS. Si le CSARS est convaincu que l'action du Service est à l'abri de tout reproche, il fait part de cette assurance au plaignant. En cas de doute, il en informe le directeur du SCRS et le solliciteur général et, dans la mesure du possible, il expose l'affaire dans son rapport annuel.

Au cours de 2000–2001, la majeure partie des investigations du Comité au sujet des plaintes de ce type ont révélé que le Service n'était ni mêlé aux activités prétendues par les plaignants ni responsable de ces activités.

Plaintes soustraites aux enquêtes du Comité

Le Comité a reçu 26 plaintes à l'égard desquelles il n'a pu enquêter parce qu'elles ne respectaient pas la condition énoncée à l'article 41 de la Loi, soit celle d'avoir été présentées en premier lieu au directeur du SCRS. Le CSARS répond aux plaignants en soulignant cette condition de l'article 41 et en leur fournissant l'adresse du directeur. Le Comité ne peut, non plus, examiner les plaintes des personnes qui jouissent d'un droit de recours grâce à une procédure de règlement de griefs établie en vertu de la *Loi sur le SCRS* ou de la *Loi sur les relations de travail dans la fonction publique*.

Plaintes ne relevant pas du CSARS

Le Comité a reçu 12 plaintes qui ne concernaient ni le SCRS ni des questions de sécurité nationale. En pareil cas, le CSARS informe les intéressés que leurs plaintes ne relèvent pas de lui et, si possible, il les adresse aux autorités compétentes.

PLAINTES CONCERNANT DES HABILITATIONS DE SÉCURITÉ

Le Comité a enquêté sur quatre plaintes ayant trait à des habilitations de sécurité en 2000–2001. Deux de ces dossiers, qui concernent la révocation d'habilitations, sont clos. Dans un cas la plainte a été retirée; dans l'autre, après étude, le Comité a rendu sa décision qui est résumée à l'annexe D. Les deux autres plaintes concernent des recommandations du Service de refuser l'habilitation de sécurité; les enquêtes du Comité à ce sujet sont en cours.

CONSTATATIONS CONCERNANT DES RAPPORTS MINISTÉRIELS

Refus d'attribution de citoyenneté

Dans l'interminable affaire de la demande de citoyenneté d'Ernst Zündel – dont le Comité a été saisi pour la première fois en 1995 – nous avons été informés en décembre 2000 que l'intéressé avait retiré sa demande et que Citoyenneté et Immigration Canada avait accepté son retrait. Par suite de ce fait nouveau, il n'y avait plus de raison de poursuivre l'enquête. Le CSARS ne présentera donc pas au gouverneur en conseil le rapport prévu au paragraphe 19(6) de la *Loi sur la citoyenneté.*

Rapports en vertu de la *Loi sur l'immigration*

Le Comité n'a reçu du Ministre aucun rapport de ce type au cours de la période à l'étude. Comme il le mentionnait dans son rapport de l'an dernier, il a été appelé en mars 2000 à réexaminer une affaire concernant une décision qu'il avait rendue en 1998 (Yamani). Depuis, le CSARS a été informé que Citoyenneté et Immigration Canada avait décidé de ne pas poursuivre l'affaire. Il en est donc dessaisi.

RENVOIS DE LA COMMISSION CANADIENNE DES DROITS DE LA PERSONNE

La Commission canadienne des droits de la personne n'a saisi le Comité d'aucune affaire au cours de la période à l'étude. Une enquête qui avait été portée devant le CSARS au cours du précédent exercice a par contre été menée à terme et a fait l'objet d'un rapport à la Commission.

Section 3

Régime de responsabilisation du SCRS

Régime de responsabilisation du SCRS

Le Service, qui est un organisme du gouvernement du Canada, doit rendre compte au Parlement et à la population du Canada par l'entremise du solliciteur général. En raison du sérieux de ses activités et du degré d'intrusion qu'elles peuvent comporter, les mécanismes prévus par la loi pour assurer cette reddition de compte sont rigoureux et multidimensionnels. Au sein du SCRS et à l'extérieur, il existe un certain nombre de systèmes indépendants qui permettent de scruter les activités du Service et de voir si elles sont conformes à son mandat.

La nouvelle publication du Bureau du Conseil privé intitulée *La collectivité canadienne de la sécurité et du renseignement*, Ottawa, 2001, fournit une description complète de l'appareil canadien du renseignement de sécurité et des systèmes de reddition de compte dont il est assorti.

L'une des tâches du CSARS – lui-même un des éléments du régime – est d'évaluer le fonctionnement des rouages de la responsabilisation du SCRS à l'endroit du ministre dont il relève et de formuler des observations à cet égard.

A. Les rouages de la responsabilisation du SCRS

LES INSTRUCTIONS DU MINISTRE

En vertu du paragraphe 6(2) de la *Loi sur le SCRS*, le Ministre peut donner des instructions au sujet des activités et des enquêtes du Service. Le Comité est expressément chargé d'examiner toute nouvelle instruction. Au cours de l'exercice 2000 – 2001, le Ministre a diffusé un nouveau recueil d'instructions revues et mises à jour qui remplacent intégralement les précédentes. Ce recueil, qui fait l'objet d'une étude spéciale du CSARS, est examiné en détail à la page 8.

CHANGEMENTS AUX POLITIQUES OPÉRATIONNELLES DU SERVICE

Au cours de l'exercice 2000–2001, le Service a élaboré deux nouvelles politiques, l'une sur la préparation des évaluations de menaces et l'autre sur l'emploi du polygraphe dans les opérations du SCRS. Il en a modifié quatorze autres, soit pour tenir compte de changements apportés aux instructions du Ministre, soit pour les harmoniser avec les usages courants.

COMMUNICATIONS POUR RAISONS D'INTÉRÊT PUBLIC ET NATIONAL

L'article 19 de la *Loi sur le SCRS* interdit au Service de communiquer des informations recueillies au cours d'enquêtes, sauf si des circonstances particulières

l'exigent. En vertu de l'alinéa 19(2)d), le Ministre peut l'autoriser à faire de telles communications « pour des raisons d'intérêt public ». Selon la Loi, le directeur du SCRS est tenu de présenter au Comité un rapport ayant trait à toute communication faite pour de telles raisons.

Le Service a fait un rapport à ce sujet en 2000–2001. Les informations en cause, communiquées à un avocat représentant un ministre, avaient trait à une ébauche d'affidavit qu'un employé du Service avait rédigée relativement à une poursuite judiciaire.

De plus, à titre de mandataire du Ministre, le SCRS peut, « pour des raisons d'intérêt national », communiquer des renseignements dans des circonstances particulières. Selon la politique du Service, le Comité doit être informé de toute communication semblable, mais il n'y en pas eu au cours de l'exercice considéré.

RÈGLEMENTS ET NOMINATIONS PAR LE GOUVERNEUR EN CONSEIL

Aux termes du paragraphe 8(4) de la *Loi sur le SCRS*, le gouverneur en conseil peut imposer au Service des règlements visant les pouvoirs et fonctions de son directeur ainsi que la conduite et la discipline de ses employés. Le gouverneur en conseil n'a établi aucun règlement semblable en 2000–2001.

CERTIFICAT DE L'INSPECTEUR GÉNÉRAL

L'inspecteur général du SCRS relève du solliciteur général et joue effectivement pour lui le rôle de vérificateur interne en scrutant les activités opérationnelles du Service et en s'assurant que celui-ci se conforme à ses politiques et à la loi. Chaque année, l'inspecteur général doit remettre au Ministre un certificat indiquant « dans quelle mesure le rapport [du directeur] lui paraît acceptable » quant à ces activités et l'informant de tout cas où le Service a dérogé à la Loi ou aux instructions ministérielles et de ceux où il a exercé ses pouvoirs d'une façon abusive ou inutile. Le Ministre fait transmettre ce certificat au Comité de surveillance.

L'inspecteur général actuel – nommé en juillet 1999 – a remis en novembre 2000 son premier certificat. Il y affirme que le rapport annuel du directeur au Ministre lui paraît entièrement acceptable et qu'à son avis « le Service n'a pas accompli d'actes non autorisés en vertu de la Loi, n'a pas contrevenu aux instructions données par le ministre et n'a pas exercé ses pouvoirs d'une façon abusive ou inutile ».

L'inspecteur général ajoute qu'il a convenu avec le directeur du SCRS que le rapport de celui-ci devra à l'avenir être plus concis et ciblé. Ce document décrira « les points

saillants des activités du Service pour la période visée [et... fera] état de questions graves ayant trait aux activités opérationnelles, à la politique d'intérêt public, à une controverse possible et aux défis que pourrait représenter la réalisation du mandat du Service ». D'autres données détaillées pourront être examinées par le solliciteur général adjoint, par le Bureau de l'inspecteur général et par le Comité de surveillance.

L'autre question dont traite l'inspecteur général concerne une attestation de sécurité que le ministre de la Citoyenneté et de l'Immigration et le solliciteur général avaient signée à la suite d'un rapport du Service sur des renseignements de sécurité. Dans une décision ultérieure, la Cour fédérale a annulé le certificat, le jugeant « non raisonnable ».

Après avoir lui-même évalué ce rapport du SCRS, l'inspecteur général a conclu que c'était un compte rendu justifié d'une affaire exacte et crédible et qu'il répondait au critère des « motifs raisonnables de croire », énoncé au paragraphe 19(1) de la *Loi sur l'immigration*. Il s'est en outre dit favorable aux initiatives prises par le Service pour que ses futurs rapports sur des renseignements de sécurité soient « plus convaincants lorsqu'ils sont présentés à la Cour ».

AGISSEMENTS ILLICITES

Aux termes du paragraphe 20(2) de la *Loi sur le SCRS*, le directeur du Service doit faire rapport au Ministre s'il estime qu'un employé peut avoir commis un acte illicite dans l'exercice de ses fonctions. Le cas échéant, le Ministre transmet alors ce rapport au procureur général du Canada et au Comité, accompagné de ses observations.

En 2000–2001, nous avons reçu un rapport semblable signalant le cas d'un employé du SCRS qui pourrait avoir commis un acte illicite. Au moment de mettre sous presse, le procureur général n'avait pas encore rendu sa décision au sujet de cette affaire. Dans son rapport de l'an dernier, le Comité avait fait état d'une affaire non réglée d'acte illicite, remontant à 1997. Depuis, le procureur général a décidé de ne pas intenter de poursuite.

ENQUÊTES EN VERTU DE L'ALINÉA 2D)

Selon les instructions du Ministre, celui-ci doit autoriser toute enquête sur les menaces à la sécurité du Canada, au sens de l'alinéa 2d) de la *Loi sur le SCRS* – souvent appelé clause sur la « subversion ». Aucune enquête semblable n'a été autorisée en 2000–2001.

B. Au sein du CSARS

SUIVI DES QUESTIONS OFFICIELLES

Dans l'exercice de son rôle de surveillance, le Comité demande des renseignements et des documents au SCRS au sujet de ses activités. Au cours de l'exercice 2000–2001 (du 1er avril 2000 au 31 mars 2001), il lui a ainsi posé 91 questions officielles, outre celles ayant trait aux dossiers de plaintes.

Le Comité demande souvent à titre officieux d'autres renseignements au SCRS. Au cours de l'exercice considéré, le Service a répondu avec diligence à ces demandes, parfois urgentes.

ACTIVITÉS DE RECHERCHE ET D'EXAMEN

À l'Administration centrale du SCRS, un bureau séparé et des ordinateurs sont mis à la disposition du personnel et des membres du Comité, pour leur usage exclusif. Les recherchistes et les analystes du CSARS, qui rendent compte régulièrement à la haute direction, répartissent leur temps entre leurs propres bureaux et les locaux que le Service met à leur disposition.

SÉANCES D'INFORMATION

Aux réunions mensuelles du Comité, la présidente et les membres rencontrent les autorités gouvernementales pour maintenir les ponts et se tenir au courant des faits nouveaux. Lorsque les membres du CSARS se réunissent à l'extérieur d'Ottawa, ils profitent de l'occasion pour visiter les bureaux régionaux du SCRS. En juin 2000 et en février 2001, ils ont ainsi rencontré les cadres supérieurs du bureau régional du SCRS à Toronto et, en septembre 2000, ceux du bureau de Montréal. Les autres réunions du Comité ont eu lieu à Ottawa.

NOMINATION DE CADRES SUPÉRIEURS AU CSARS

En décembre 2000, le directeur exécutif du Comité, Mme Susan Pollak, a annoncé la nomination de M. Thomas Dastous au poste d'avocat principal du CSARS. M. Dastous était au ministère fédéral de la Justice.

En janvier 2001, Mme Kelly McGee est entrée au CSARS à titre de directrice de la recherche. Auparavant, elle dirigeait les Services législatifs et d'élaboration de la politique à la Municipalité régionale d'Ottawa-Carleton.

AUTRES ACTIVITÉS DU COMITÉ

- En septembre 2000, la présidente, le directeur exécutif, le sous-directeur exécutif et l'avocat principal ont rencontré à Ottawa le nouvel inspecteur

général du Renseignement d'Afrique du Sud pour discuter du rôle et des fonctions du Comité de surveillance des activités de renseignement de sécurité au sein du régime politique canadien.

- En octobre 2000, une délégation du Danemark a rencontré la haute direction du Comité pour étudier le mandat et les activités du CSARS. Elle menait alors des recherches dans le cadre d'une commission chargée d'examiner les services de renseignement danois.
- Le conseiller en matière de sécurité nationale auprès du président du Mexique Vicente Fox a rencontré le directeur exécutif, le sous-directeur exécutif et l'avocat principal en février 2001 pour étudier le mandat, la structure et les activités du CSARS ainsi que l'expérience acquise au fil des 16 dernières années.
- En mars 2001, les membres du Comité norvégien d'examen du renseignement, de la surveillance et de la sécurité ont rencontré la haute direction du CSARS dans le cadre d'un voyage d'études en Amérique du Nord. Pour ce comité, le modèle du CSARS revêt un intérêt spécial parmi les organismes semblables qu'il a étudiés.

SITE WEB

Au cours de l'exercice 2000–2001, on a remanié considérablement le site Web du CSARS (*www.sirc-csars.gc.ca*) pour en faire une source d'information plus attrayante et plus conviviale à l'intention des Canadiens. Cet outil repensé donne accès à tous les rapports annuels du Comité depuis sa création, en 1984. On y trouve les toutes dernières nouvelles sur les activités du CSARS ainsi que diverses informations allant des notices biographiques des membres à la procédure à suivre pour porter plainte au sujet d'une activité du SCRS ou du refus d'une habilitation de sécurité. Au cours de l'exercice 2000–2001, le site a accueilli 543 137 visiteurs, soit quelque 45 000 par mois ou 1 500 par jour.

BUDGET ET DÉPENSES

Le Comité continue de contenir ses activités dans les limites des ressources établies en 1985. Pendant l'exercice 2000–2001, il a de nouveau enregistré une hausse marquée du nombre d'affaires quasi judiciaires (plaintes), ce qui s'est répercuté sur ses dépenses non discrétionnaires (voir le tableau X).

Voici les autres postes de dépenses importants :

- les mises à niveau de l'infrastructure informatique interne visant à la conformer aux normes actuelles à respecter sur le plan opérationnel et en matière de

Tableau 4
Dépenses du CSARS

	2001–2002 (prévues)	2000–2001 (réelles)	1999–2000 (réelles)
Personnel	1 112 000	837 623	841 945
Biens et services	962 000	953 592	821 055
Total	2 074 000	1 792 295	1 663 000

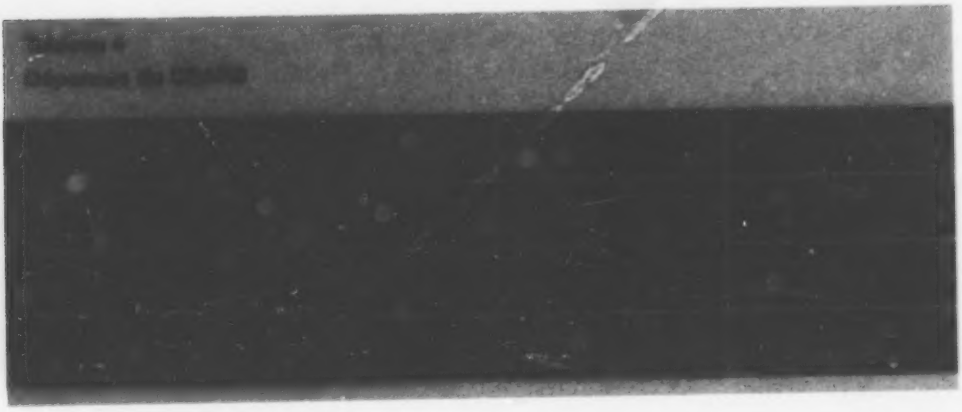
sécurité pour traiter de grandes quantités d'informations d'un niveau de classification élevé;

- la modernisation du système de traduction simultanée dont est dotée la salle d'audience du Comité;
- l'amélioration des locaux auxquels le public a accès et des salles d'audience afin de les rendre plus accueillants et plus fonctionnels;
- les frais de déplacement au Canada pour les audiences du Comité et pour la recherche nécessaire aux vérifications; et
- les traitements et avantages du personnel.

PERSONNEL ET ORGANISATION

Le Comité a un effectif de 16 employés : un directeur exécutif, un sous-directeur exécutif, un avocat principal, un avocat, un agent chargé des plaintes (accès à l'information et protection des renseignements personnels (AIPRP)), un parajuriste principal/greffier d'audience, un directeur de la recherche, un conseiller principal en matière de politiques, quatre analystes de la recherche, un agent financier et administrateur, un adjoint administratif et deux employés de soutien. Ces derniers sont chargés de mettre en œuvre les mesures de sécurité spéciales qui permettent au CSARS de traiter les documents délicats portant une cote de sécurité élevée.

Aux réunions mensuelles du Comité, les membres déterminent officiellement les travaux de recherche et les autres tâches qu'ils veulent effectuer et ils fixent les priorités à l'intention du personnel. La marche des activités courantes est confiée au directeur exécutif qui s'enquiert, au besoin, de la ligne de conduite à tenir auprès de la présidente, première dirigeante du CSARS.



sécurité pour traiter de grandes quantités d'informations d'un niveau de classification élevé;

- la modernisation du système de traduction simultanée dont est dotée la salle d'audience du Comité;
- l'amélioration des locaux auxquels le public a accès et des salles d'audience afin de les rendre plus accueillants et plus fonctionnels;
- les frais de déplacement au Canada pour les audiences du Comité et pour la recherche nécessaire aux vérifications; et
- les traitements et avantages du personnel.

PERSONNEL ET ORGANISATION

Le Comité a un effectif de 16 employés : un directeur exécutif, un sous-directeur exécutif, un avocat principal, un avocat, un agent chargé des plaintes/accès à l'information et protection des renseignements personnels (AIPRP), un parajuriste principal/greffier- audiencier, un directeur de la recherche, un conseiller principal en matière de politiques, quatre analystes de la recherche, un agent financier et administrateur, un adjoint administratif et deux employés de soutien. Ces derniers sont chargés de mettre en œuvre les mesures de sécurité spéciales qui permettent au CSARS de traiter les documents délicats portant une cote de sécurité élevée.

Aux réunions mensuelles du Comité, les membres déterminent officiellement les travaux de recherche et les autres tâches qu'ils veulent effectuer et ils fixent les priorités à l'intention du personnel. La marche des activités courantes est confiée au directeur exécutif qui s'enquiert, au besoin, de la ligne de conduite à tenir auprès de la présidente, première dirigeante du CSARS.

Annexe A

Sigles employés dans le rapport

Sigles employés dans le rapport

ALS	Agent de liaison-sécurité
AT	Antiterrorisme
CARC	Comité d'approbation et de réévaluation des cibles
CE	Contre-espionnage
CER	Comité d'évaluation du renseignement (Bureau du Conseil privé)
CIC	Citoyenneté et Immigration Canada
Comité	Comité de surveillance des activités de renseignement de sécurité (CSARS)
CPPR	Comité principal de production de renseignements
CSARS	Comité de surveillance des activités de renseignement de sécurité
CST	Centre de la sécurité des télécommunications (MDN)
Directeur	Le directeur du SCRS
EAP	Direction des exigences, de l'analyse et de la production (SCRS)
GRC	Gendarmerie royale du Canada
SCRS	Service canadien du renseignement de sécurité
Service	Service canadien du renseignement de sécurité (SCRS)

Annexe B

Rapports et études du CSARS depuis 1984

Rapports et études du CSARS depuis 1984

(Les rapports présentés aux termes de l'article 54, soit les rapports spéciaux du Comité au Ministre, sont marqués d'un astérisque.)

1. *Dix-huit mois après la séparation : une appréciation de la conception du SCRS sur le recrutement, le perfectionnement et les questions connexes,* (SECRET) * (86/87- 01)

2. *Rapport d'une étude portant sur le filtrage de sécurité des fonctionnaires et des personnes postulant un emploi dans la fonction publique fédérale,* (SECRET) * (86/87-02)

3. *Le réseau du renseignement et de sécurité au sein de l'administration gouvernementale du Canada : une description,* (SECRET) * (86/87-03)

4. *Alerte de sécurité à l'aéroport d'Ottawa,* (SECRET) * (86/87-05)

5. *Report to the Solicitor General of Canada Concerning CSIS' Performance of its Functions,* (SECRET) * (87/88-01)

6. *Pour corriger une situation : langues officielles et relations de travail au sein du SCRS,* (NON CLASSIFIÉ) * (86/87-04)

7. *Counter-Subversion: SIRC Staff Report,* (SECRET) (87/88-02)

8. *Rapport du CSARS – Sélection des immigrants,* (SECRET) * (87/88-03)

9. *L'usage par le SCRS de ses pouvoirs d'enquête en ce qui concerne le mouvement ouvrier,* (VERSION PUBLIQUE) * (87/88-04)

10. *La Direction de l'évaluation du renseignement : une revue par le CSARS du processus de production,* (SECRET) * (88/89-01)

11. *CSARS – Examen du programme de l'antiterrorisme du SCRS,* (TRÈS SECRET) * (88/89-02)

12. *Rapport présenté au Solliciteur général du Canada sur la protection des biens scientifiques et techniques au Canada : le rôle du SCRS*, (SECRET) * (89/90-02)

13. *SIRC Report on CSIS Activities Regarding the Canadian Peace Movement*, (SECRET) * (89/90-03)

14. *L'examen de la politique et des pratiques du SCRS concernant les divulgations non autorisées d'informations classifiées*, (SECRET) (89/90-04)

15. *Report to the Solicitor General of Canada on Citizenship/Third Party Information*, (SECRET) * (89/90-05)

16. *Modifications à la Loi sur le SCRS : propositions au Comité spécial de la Chambre des communes*, (NON CLASSIFIÉ) (89/90-06)

17. *Rapport sur l'entrevue concernant les Innus et l'enquête sur l'extrémisme autochtone*, (SECRET) * (89/90-07)

18. *Supplement to the Committee's Report on Immigration Screening of January 18, 1988*, (SECRET) * (89/90-01)

19. *A Review of the Counter-Intelligence Program in the CSIS*, (TRÈS SECRET) * (89/90-08)

20. *Échanges de renseignements avec des organismes canadiens*, (SECRET) * (90/91-03)

21. *Cibles établies en vertu de l'alinéa 2d) – Une étude du CSARS sur les opérations restantes de la Direction de l'antisubversion*, (SECRET) (90/91-06)

22. *Études régionales (six études sur une région)*, (TRÈS SECRET) (90/91-04)

23. *Study of CSIS' Policy Branch*, (CONFIDENTIEL) (90/91-09)

24. *Enquêtes, affectation de sources et rapport sur les cibles en vertu de l'alinéa 2b)*, (TRÈS SECRET) (90/91-05)

25. *Communication de renseignements aux services étrangers*, (TRÈS SECRET) * (90/91-02)

26. *Examen par le CSARS des activités du SCRS touchant les Canadiens autochtones*, (SECRET) * (90/91-07)

27. *Enquêtes de sécurité sur les campus universitaires*, (TRÈS SECRET) * (90/91-01)

28. *Report on Multiple Targeting*, (SECRET) (90/91-08)

29. *Revue de l'enquête sur Bull, la Corporation de recherche spatiale et l'Iraq*, (SECRET) (91/92-01)

30. *Rapport sur l'immigration d'Al Mashat au Canada*, (SECRET) * (91/92-02)

31. *East Bloc Investigations*, (TRÈS SECRET) (91/92-08)

32. *Review of CSIS Activities Regarding Sensitive Institutions*, (TRÈS SECRET) (91/92- 10)

33. *CSIS and the Association for New Canadians*, (SECRET) (91/92-03)

34. *Échange d'informations et de renseignements entre le Service canadien du renseignement de sécurité et le Centre de la sécurité des télécommunications*, (TRÈS SECRET)* (91/92-04)

35. *Victor Ostrovsky*, (TRÈS SECRET) (91/92-05)

36. *Report on Two Iraqis – Ministerial Certificate Case*, (SECRET) (91/92-06)

37. *Évaluations de la menace, étude en vertu de l'article 40*, (SECRET) * (91/92-07)

38. *L'attaque contre l'ambassade de l'Iran à Ottawa*, (TRÈS SECRET) * (92/93-01)

39. *"STUDYNT" The Second CSIS Internal Security Case*, (TRÈS SECRET) (91/92-15)

40. *Les cibles du terrorisme national – Un examen du CSARS*, (TRÈS SECRET) * (90/91-13)

41. *CSIS Activities with respect to Citizenship Security Screening*, (SECRET) (91/92-12)

42. *The Audit of Section 16 Investigations*, (TRÈS SECRET) (91/92-18)

43. *Activités du SCRS pendant la Guerre du Golfe : entrevues dans la communauté*, (SECRET) (90/91-12)

44. *Examen de l'enquête menée par le SCRS sur un agent clandestin latino-américain – Un examen du CSARS*, (TRÈS SECRET) * (90/91-10)

45. *Les activités du SCRS relativement à la destruction de l'avion affecté au vol 182 d'Air India le 23 juin 1985 – Un examen du CSARS*, (TRÈS SECRET) * (91/92-14)

46. *Région des Prairies – Rapport sur les autorisations d'enquête (chapitre 1)*, (TRÈS SECRET) * (90/91-11)

47. *L'attentat contre Hassan El-Tourabi*, (SECRET) (92/93-07)

48. *Domestic Exchanges of Information* (A SIRC Review – 1991/92), (SECRET) (91/92-16)

49. *Vérification de la Région des Prairies*, (TRÈS SECRET) (90/91-11)

50. *La présumée venue du sheikh Rahman à Ottawa*, (SECRET) (AT 93-06)

51. *Regional Audit*, (TRÈS SECRET)

52. *Examen par le CSARS des bureaux des ALS du Service (Londres et Paris)*, (SECRET) (91/92-11)

53. *The Asian Homeland Conflict*, (SECRET) (CT 93-03)

54. *Intelligence - Source Confidentiality*, (TRÈS SECRET) (CI 93-03)

55. *Domestic Investigations (1)*, (SECRET) (CT 93-02)

56. *Enquêtes menées au Canada (2)*, (TRÈS SECRET) (AT 93-04)

57. *Middle East Movements*, (SECRET) (CT 93-01)

58. *A Review of CSIS' SLO Posts (1992-93)*, (SECRET) (CT 93-05)

59. *Review of Traditional CI Threats*, (TRÈS SECRET) (CI 93-01)

60. *Protecting Science, Technology and Economic Interests*, (SECRET) (CI 93-04)

61. *Domestic Exchanges of Information*, (SECRET) (CI 93-05)

62. *Foreign Intelligence Service for Canada*, (SECRET) (CI 93-06)

63. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TRÈS SECRET) (CI 93-11)

64. *Sources in Government*, (TRÈS SECRET) (CI 93-09)

65. *Regional Audit*, (TRÈS SECRET) (CI 93-02)

66. *The Proliferation Threat*, (SECRET) (CT 93-07)

67. *L'Affaire du Heritage Front, rapport présenté au Solliciteur général du Canada*, (SECRET) * (AT 94-02)

68. *A Review of CSIS' SLO Posts (1993-94)*, (SECRET) (CT 93-09)

69. *Échanges d'information avec des organismes canadiens (enquête du CSARS 1993- 1994)*, (SECRET) (CE 93-08)

70. *The Proliferation Threat - Case Examination*, (SECRET) (CT 94-04)

71. *Community Interviews*, (SECRET) (CT 93-11)

72. *Une enquête suivie en matière de contre-espionnage*, (TRÈS SECRET) * (CE 93- 07)

73. *Potential for Political Violence in a Region*, (SECRET) (CT 93-10)

74. *A SIRC Review of CSIS' SLO Posts (1994-95)*, (SECRET) (CT 95-01)

75. *Regional Audit*, (TRÈS SECRET) (CI 93-10)

76. *Terrorism and a Foreign Government*, (TRÈS SECRET) (CT 94-03)

77. *Visit of Boutros Boutros-Ghali to Canada*, (SECRET) (CI 94-04)

78. *Review of Certain Foreign Intelligence Services*, (TRÈS SECRET) (CE 94-02)

79. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TRÈS SECRET) (CI 94-01)

80. *Échanges d'information avec des organismes canadiens (enquête du CSARS 1994-1995)*, (SECRET) (CE 94-03)

81. *Alleged Interference in a Trial*, (SECRET) (CT 95-04)

82. *CSIS and a "Walk-In"*, (TRÈS SECRET) (CI 95-04)

83. *A Review of a CSIS Investigation relating to a Foreign State*, (TRÈS SECRET) (CI 95-02)

84. *The Audit of Section 16 Investigations and Foreign Intelligence Reports*, (TRÈS SECRET) (CI 95-05)

85. *Vérification régionale*, (TRÈS SECRET) (AT 95-02)

86. *A Review of Investigations of Emerging Threats*, (TRÈS SECRET) (CI 95-03)

87. *Domestic Exchanges of Information*, (SECRET) (CI 95-01)

88. *Homeland Conflict*, (TRÈS SECRET) (CT 96-01)

89. *Vérification régionale*, (TRÈS SECRET) (CE 96-01)

90. *La gestion des sources humaines*, (TRÈS SECRET) (CE 96-03)

91. *Economic Espionage I*, (SECRET) (CI 96-02)

92. *Economic Espionage II*, (TRÈS SECRET) (CI 96-02)

93. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1996-1997*, (TRÈS SECRET) (CI 96-04)

94. *Urban Political Violence*, (SECRET) (SIRC 1997-01)

95. *Domestic Exchanges of Information (1996-97)*, (SECRET) (SIRC 1997-02)

96. *Conflit étranger*, (SECRET) (CSARS 1997-03)

97. *Regional Audit*, (TRÈS SECRET) (SIRC 1997-04)

98. *CSIS Liaison with Foreign Agencies*, (TRÈS SECRET) (SIRC 1997-05)

99. *Spy Case*, (TRÈS SECRET) (SIRC 1998-02)

100. *Enquêtes menées au Canada*, (TRÈS SECRET) (CSARS 1998-03)

101. *Coopération du SCRS avec la Gendarmerie royale du Canada - Partie I*, (SECRET) * (CSARS 1998-04)

102. *Source Review*, (TRÈS SECRET) (SIRC 1998-05)

103. *Interagency Cooperation Case*, (TRÈS SECRET) (SIRC 1998-06)

104. *A Case of Historical Interest*, (TRÈS SECRET) (SIRC 1998-08)

105. *Le rôle du SCRS dans le filtrage de sécurité des demandes d'immigration*, (SECRET) (AT 95-06)

106. *Un conflit étranger - deuxième partie* (TRÈS SECRET) (CSARS 1997-03)

107. *Review of Transnational Crime* (SECRET) (SIRC 1998-01)

108. *Coopération du SCRS avec la GRC - Partie II*, (SECRET) * (CSARS 1998-04)

109. *Audit of Section 16 Investigations & Foreign Intelligence 1997-98* (TRÈS SECRET) (SIRC 1998-07)

110. *Review of Intelligence Production* (SECRET) (SIRC 1998-09)

111. *Regional Audit* (TRÈS SECRET) (SIRC 1998-10)

112. *CSIS Liaison with Foreign Agencies* (TRÈS SECRET) (SIRC 1998-11)

113. *Allégations d'un ancien employé du SCRS*, (TRÈS SECRET) * (CSARS 1998-12)

114. *CSIS Investigations on University Campuses* (SECRET) (SIRC 1998-14)

115. *Review of Foreign Intelligence Activities in Canada* (TRÈS SECRET) (SIRC 1998-15)

116. *Files* (TRÈS SECRET) (SIRC 1998-16)

117. *Audit of Section 16 Investigations & Foreign Intelligence* (TRÈS SECRET) (SIRC 1999-01)

118. *A Long-Running Counter Intelligence Investigation* (TRÈS SECRET) (SIRC 1999-02)

119. *Domestic Exchanges of Information* (TRÈS SECRET) (SIRC 1999-03)

120. *Proliferation* (TRÈS SECRET) (SIRC 1999-04)

121. *Observation du CSARS sur le projet de loi C-31 dont est actuellement saisi le Parlement* (PROTÉGÉ) * (CSARS 1999-05)

122. *Domestic Targets* (TRÈS SECRET) (SIRC 1999-06)

123. *Terrorist Fundraising* (TRÈS SECRET) (SIRC 1999-07)

124. *Regional Audit* (TRÈS SECRET) (SIRC 1999-08)

125. *Foreign State Activities* (TRÈS SECRET) (SIRC 1999-09)

126. *Project Sidewinder* (TRÈS SECRET) (SIRC 1999-10)

127. *Security Breach* (TRÈS SECRET) (SIRC 1999-11)

128. *Domestic Exchanges of Information 1999-2000* (TRÈS SECRET) (SIRC 2000-01)

129. *Audit of Section 16 Investigations and Foreign Intelligence Reports 1999-2000* (TRÈS SECRET) (SIRC 2000-02)

130. *CSIS Liaison with Foreign Agencies* (TRÈS SECRET) (SIRC 2000-03)

131. *Regional Audit* (TRÈS SECRET) (SIRC 2000-04)

132. *Warrant Review* (TRÈS SECRET) (SIRC 2000-05)

133. *Review of CSIS Briefs to Citizenship and Immigration Canada 1999-2000* (TRÈS SECRET (SIRC 2001-02)

Annexe C

Recommandations et principales constatations

Recommandations et principales constatations

LIAISON DU SCRS AVEC LES ORGANISMES ÉTRANGERS

L'examen du CSARS a porté sur un bureau d'agent de liaison-sécurité (ALS) qui œuvre à l'étranger dans un milieu particulièrement difficile. C'est un défi de taille d'assurer la sécurité du cadre physique de fonctionnement de ce bureau où les conditions de travail généralement pénibles empirent la situation. Au cours de sa vérification, le Comité a été frappé par les piètres conditions dans lesquelles le personnel du Service doit travailler. Des installations déficientes, combinées à la lourde charge de travail occasionnée par la multiplication des demandes d'immigration et de visa requérant un filtrage de sécurité, suscitent un climat défavorable. En dépit de ces circonstances difficiles, l'ALS et le personnel de ce bureau canadien font du bon travail.

Nous avons constaté que, même si l'ALS a fait des progrès constants auprès des interlocuteurs étrangers, il lui reste moins de temps pour nouer des relations avec les autres pays dont il est théoriquement chargé dans la région, étant donné que le volet immigration de son mandat l'accapare de plus en plus.

La charge de travail manifestement trop lourde a fait craindre au Comité que certaines fonctions importantes du bureau puissent ne pas être remplies promptement. La haute direction du Service a dit au CSARS qu'elle partageait ces craintes et qu'à son avis ce problème, côté immigration, était commun à certains autres bureaux d'ALS. Le Comité est d'avis que le SCRS voudra peut-être scruter cet élément de son Programme de liaison avec l'étranger.

Le Comité a examiné toue la documentation ayant trait à la coopération opérationnelle et aux échanges d'informations auxquels avait pris part le bureau d'ALS entre le 31 mars 1998 et le 30 juin 2000. Il y a relevé un seul échange problématique. Nous avons dit au Service qu'il devrait songer à transmettre les renseignements mis à jour à ses clients de façon qu'ils puissent replacer son opinion antérieure dans le bon contexte.

La crainte de répercussions sur le plan des droits de la personne était à l'avant-plan de la vérification de ce bureau par le Comité. Les ALS sont tenus de fournir au reste du SCRS des évaluations exactes et à propos sur la réputation des organismes, et cela, sur deux plans : le respect des droits de la personne et la tendance à transmettre

sans autorisation ces informations à des tiers. Pour ce qui est du bureau d'ALS soumis à la vérification, le Comité n'a trouvé aucun échange d'informations qui ne respectait pas ces normes et il est convaincu que toutes les évaluations d'organismes en matière de respect des droits de la personne ont été effectuées selon les règles de l'art.

LES INSTRUCTIONS DU MINISTRE – RÉVISION ET MISE À JOUR

En février 2001, le solliciteur général a diffusé un recueil d'instructions ministérielles révisées sur la gestion du Service – ce que le Comité souhaitait depuis un certain temps déjà.

Le nouveau recueil (document classifié) rationalise passablement l'orientation stratégique du Service par le gouvernement et, de l'avis du Comité, témoigne d'une maturation du cadre légal et stratégique qui régit le travail du SCRS. Les directives ministérielles sont désormais considérablement simplifiées et uniformes quant au langage employé et forment un document concis et cohérent. Il est en outre manifeste qu'il y a eu, quant à la gestion courante du SCRS, un transfert global de pouvoirs discrétionnaires du cabinet du solliciteur général au directeur du Service. Lors de vérifications futures, le Comité compte porter une attention particulière à la manière dont les nouvelles instructions seront interprétées et appliquées à l'ensemble des activités du Service.

ÉCHANGES D'INFORMATIONS AU CANADA (5)

Le Comité a examiné tous les échanges d'informations du Service avec les autres organismes canadiens pendant l'exercice 1999–2000. Il a en outre scruté sur place les pratiques suivies dans un bureau régional du SCRS en matière d'échanges.

Pour la période à l'étude, le Comité a relevé deux échanges préoccupants. Dans le premier cas, la base de données dans laquelle le Service avait versé les informations non sollicitées contenait plusieurs documents concernant des personnes et des organisations sur lesquelles il n'était pas autorisé à enquêter. Nous avons demandé au SCRS pourquoi il avait conservé ces documents et ses explications nous ont satisfaits. Le Comité croit toutefois que les raisons de conserver des informations non sollicitées d'une telle nature devraient, à l'avenir, être énoncées clairement dans les rapports opérationnels pertinents.

> **Le Comité recommande que les raisons pour lesquelles des informations sont conservées dans une catégorie générale soient énoncées clairement dans les rapports opérationnels.**

Le deuxième cas concernait l'opportunité de conserver certaines informations, reçues d'un organisme canadien, qui avaient trait aux activités d'un petit groupe de mineurs. Le Service a décidé par la suite qu'aucune autre mesure ne s'imposait, mais il a conservé dans ses dossiers les informations reçues initialement. Le Comité est d'avis que ces informations devraient être retirées des dossiers. Le SCRS a convenu de modifier ses rapports opérationnels de manière à refléter sa décision finale selon laquelle les informations ne justifiaient aucune autre mesure de sa part.

Le Comité recommande que le Service fasse preuve d'une plus grande diligence lorsqu'il décide s'il doit conserver des informations non sollicitées.

NOTES D'ÉVALUATION DE SÉCURITÉ À CIC

Le Comité a examiné un échantillon d'enquêtes de sécurité à l'immigration menées par le Service et choisies à partir des 166 notes d'information que le SCRS avait envoyées à CIC au cours de l'exercice 1999–2000. Il a étudié ces notes et toutes les pièces justificatives concernant chaque enquête. Toutes les notes d'information dans lesquelles le Service avait donné une opinion à CIC ont été jugées exactes et bien fondées sur les renseignements recueillis.

Le Comité a appris récemment que le Service et CIC avaient instauré le programme « Filtrage dès le début du processus » pour les demandeurs du statut de réfugié au Canada. L'objet du programme est d'éviter que l'on puisse entrer au Canada et y demeurer pendant une période indéfinie sans subir d'évaluation de filtrage de sécurité – ce qui posait un risque important selon la procédure en place lors d'un examen antérieur du Comité.

Annexe D

Résumé des plaintes

Résumé des plaintes

Voici un résumé des plaintes dont le Comité de surveillance a été saisi au cours du dernier exercice financier et qui ont donné lieu à des décisions. Ne sont pas mentionnées celles qui ont fait l'objet d'un examen administratif, qui ont été présentées au CSARS par erreur ou qu'on a jugées comme débordant son mandat.

S'il y a lieu, l'examen des plaintes par le Comité se fait au cours d'audiences quasi judiciaires que préside l'un de ses membres. Une fois les audiences terminées, celui-ci rend sa décision qui est communiquée au solliciteur général et au directeur du SCRS. La décision est aussi transmise au plaignant après suppression de toute information ayant des incidences sur le plan de la sécurité nationale.

Le Comité a fait rapport de deux décisions rendues pendant la période à l'étude : l'une concerne une affaire ayant trait à l'article 42 (refus d'une habilitation de sécurité) et l'autre, une plainte portée en vertu de l'article 41 – « activités ».

AFFAIRE N° 1

Le plaignant est un ancien employé du Service dont l'habilitation de sécurité avait été révoquée en 1999, entraînant son licenciement. Il avait alors présenté une plainte pour refus d'une habilitation de sécurité par le SCRS.

Dans ses explications visant à justifier la révocation de l'habilitation, le Service a affirmé que l'employé n'avait pu empêcher la communication de renseignements classifiés aux médias d'information et que, de ce fait, il avait violé le serment professionnel prêté par tous les employés du SCRS. Comme il faut une habilitation de sécurité pour travailler au Service, le licenciement a été immédiat.

Le plaignant a soutenu que rien ne justifiait la position du Service au sujet de la communication de renseignements : il s'était mis en rapport avec les médias afin de discuter d'une plainte portée contre le SCRS pour discrimination. Le plaignant a soulevé des doutes quant à la minutie de l'enquête du Service dans cette affaire et il a en outre affirmé que son licenciement visait à camoufler des erreurs du Service.

L'enquête du Comité n'a révélé aucune information corroborant les prétentions du plaignant. L'opération du SCRS visée par la communication était une activité licite qui était conforme aux politiques et à la loi. Même si le Service avait fait des erreurs dans la conduite de l'opération, cela ne déchargeait pas l'employé de sa responsabilité de protéger les renseignements classifiés, de l'avis du Comité.

Quant à l'enquête du Service sur la communication non autorisée, notre propre examen a révélé que la décision du directeur de révoquer l'habilitation de sécurité du plaignant était fondée sur des renseignements incomplets. Néanmoins, le Comité a trouvé que le directeur avait en mains des informations justifiant une telle décision.

Comme l'emploi du plaignant au SCRS nécessitait une habilitation de sécurité de niveau III, son licenciement consécutif à la révocation de l'habilitation de sécurité était inévitable. Le Comité a toutefois recommandé que le Service facilite la réaffectation de l'intéressé dans un autre ministère, conformément à la Politique du gouvernement sur la sécurité. Il a en outre recommandé que le Service réexamine certaines de ses méthodes et sa procédure de gestion de l'information.

AFFAIRE Nº 2

Selon une plainte déposée en vertu de l'article 41 de la Loi, son auteur affirme qu'une opération particulière du Service l'a mis à nu devant des individus dangereux, qu'un agent du SCRS a eu à son endroit un comportement menaçant et intimidant qui lui a occasionné des tensions et une anxiété indus et que le Service a fait la sourde oreille à ses demandes d'aide. Le plaignant a aussi réclamé des dommages-intérêts pour perte de revenu.

Le Comité n'a rien trouvé qui corrobore les allégations du plaignant. Aucun élément ne prouve que le Service ait mis le plaignant en danger ou ait eu à son égard un comportement menaçant ou intimidant. Le plaignant a admis au Comité que l'agent du Service n'avait pas, en fait, eu un tel comportement à son endroit. Le CSARS a en outre conclu qu'il n'y avait aucun motif de recommander le remboursement du revenu perdu.

Même s'il a jugé que la plainte était dénuée de fondement, le Comité a aussi relevé, de la part du Service, des problèmes sérieux dans la supervision de l'opération en cause. Il lui a fait diverses recommandations visant à améliorer la gestion et la procédure à suivre pour les opérations futures de ce type.